Kansas Information Technology Executive Council (ITEC)

ITEC Policy # 5200 Public Key Infrastructure Certificate Policy

ATTACHMENT 1

Certificate Policy

for the

State of Kansas

Public Key Infrastructure

Version 1.0
July, 2001

Table of contents

6 Technical security controls

7 Certificate and CRL profiles

8 Policy administration

1 Introduction

1.1 Overview

This certificate policy (this policy or CP) states the rules governing the issuance and use of certificates among those persons and devices authorized to participate in the public key infrastructure (PKI) described by this policy.

This PKI is intended to support digital signatures, encryption and access control applications in the following electronic environments:

- communications and transactions within, between and/or among agencies, departments, units and/or organizations which are a part of any governmental body (government agencies);

- communications and transactions among or between government agencies and other persons, as defined by Kansas law. Under the Kansas uniform electronic transactions act "person" means an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation or any other legal or commercial entity. Communications among persons regarding the following are covered:

  government;
  health care;
  health plans; and
  other subjects in the health care sector;
  universities;
  colleges;
  teaching and research;
  students and others in the academic sector;
  consumer activities; and
  any other purpose not specified above.

In particular, this policy describes the relationships within the PKI, among and between:

- persons in their capacity as subscribers to certificates;

- persons in their capacity as parties relying upon certificates issued under this policy (relying parties);

- a registered certification authority (registered CA) under this policy;

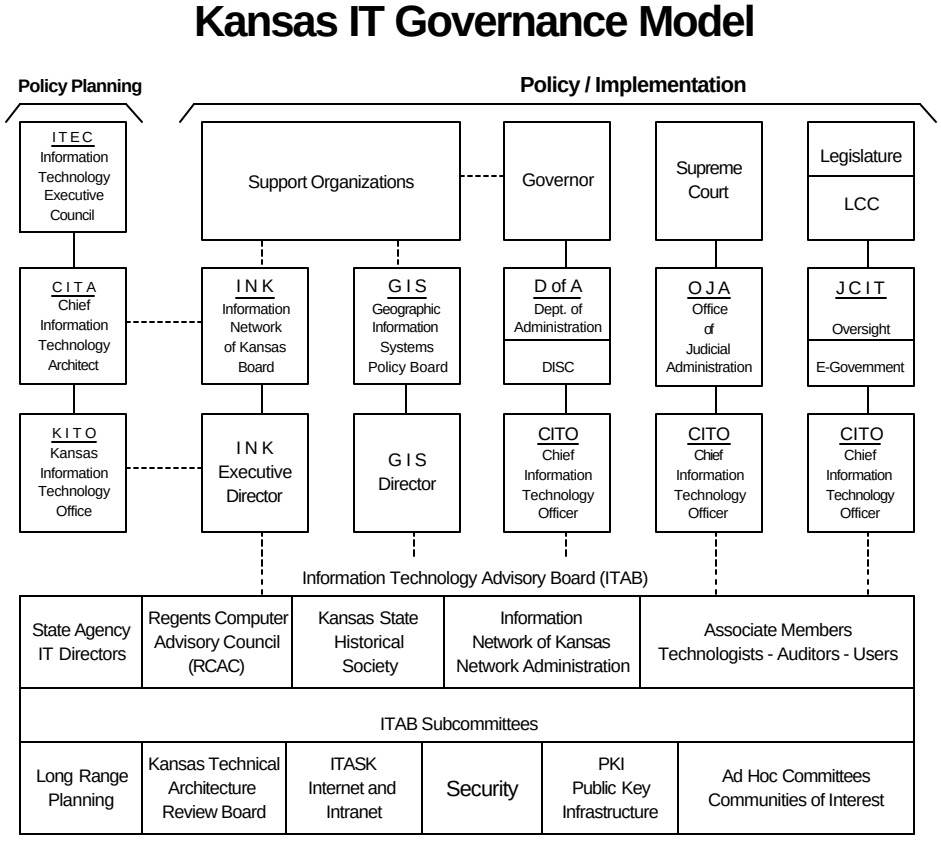
- persons acting as repositories or certificate manufacturing authorities (CMA) under this policy;

- persons acting in the capacity of authenticating registration authorities (RA) under this policy; and

- the State of Kansas. PKI and the Kansas consolidated IT governance structure are organized as follows:

PKI and the Kansas Consolidated IT Governance Structure

The Kansas IT governance structure, established in 1998 (KSA-75 7201 *et seq.*), unifies and consolidates the IT community in Kansas government. The governance model is designed so that each part of the community is made stronger by the presence of the other components.



ITAB This consolidated model features the information technology advisory board as the foundation. The operational philosophy is both bottom-up and top-down with communication among the participants vertically and horizontally. The ITAB board and sub-committees form the nucleus where many IT initiatives and projects are identified. The need for certain IT policies have genesis in ITAB as well. ITAB membership comes from state agency IT directors, regents' university IT directors (regents computer advisory council-RCAC), leadership of INK, the state historical society and associate members including, technologists, functional users, subject matter experts and others in the IT field. The ITAB will establish a PKI subcommittee to monitor the development and implementation of PKI technology in state government and will serve in an advisory role to the ITEC on PKI issues and policy.

ITEC As set forth in KSA 75-7201 *et seq.* the information technology executive council (ITEC) is comprised of seventeen members coming from both state and local government and the private sector. Private sector membership is by gubernatorial appointment. The secretary of administration in the executive branch chairs ITEC. ITEC is charged with:

- IT policies, procedures, and data management standards for the enterprise

- ✍ project management methodologies and project manager certification
- ✍ enterprise information technology architecture
- ✍ strategic information technology management plans for state agencies.

The ITEC, with an enterprise-wide view of information technology, is the most appropriate owner of policy relating to PKI implementation in Kansas.

CITA The state chief information technology architect (CITA) reports to ITEC and is secretary of ITEC. The CITA is responsible for the Kansas statewide technical architecture (KSTA), strategic information management (SIM) plan, IT project management standards, and IT policy development. The CITA will aid in the management and maintenance of the PKI certificate policy.

KITO The Kansas information technology office (KITO) supports ITEC and the CITA, in day-to-day activities, by preparing reports, plans, and policies and performing tasks necessary to conduct council business. Additionally, the KITO provides support to the CITOs in their role of project oversight, agency three-year IT plans, and project management training. The KITO will provide guidance and support for the implementation of the PKI certificate policy and oversight in regard to PKI registration authorities.

CITO The Kansas IT governance structure provides for a chief information technology officer (CITO) for each of the three branches of Kansas government. The executive branch CITO reports to the secretary of administration who, then, in turn, reports to the governor. The judicial branch CITO reports to office of judicial administrator and then the supreme court. The legislative CITO reports to the joint legislative committee on information technology (JCIT) and then to the legislative coordinating council (LCC), comprised of members from the legislature. Each CITO fills the implementation role in the model within their respective branch and has significant input in policy direction. The CITOs will be responsible for implementation of the PKI Certificate Policy and related activities within their respective branches of government.

Certificates issued under this policy may be used:

- ? to verify digital signatures;
- ? to encrypt and authenticate electronic communications;
- ? to provide evidence of identity in order to support access controls established by relying parties to prevent unauthorized access to computer systems and electronic information and documents under conditions established by such relying parties.

1.1.1 Policy overview

The PKI governed by this policy makes use of CAs registered under the laws of the State of Kansas. Subscribers and relying parties not located in the State of Kansas may obtain and/or rely upon certificates issued under this policy, and such certificates may be used for transactions, applications and communications outside the State of Kansas, provided that the laws of the State of Kansas are applied as a matter of law, unless prohibited by federal law.

1.1.1.1 State registration of CAs

Registered CAs under this policy are required to be registered in accordance with the Kansas uniform electronic transaction act (Kansas UETA), codified as KSA 16-1601 *et*

seq., particularly KSA 16-1617 – KSA 16-1619.

1.1.1.2 Identity assurance and certificate types

This policy provides for four (4) types of certificates. One factor that differentiates each type is the degree of assurance relating to the subscriber's identity that is provided by (i) the procedures used to identify and authenticate (I&A) the subscriber prior to issuance of the certificate (I&A procedures) and (ii) the degree of security a subscriber is required to use to protect his/her private key under this policy (subscriber security obligations). The four certificate types are designated high, medium, basic and rudimentary.

Security and convenience considerations must be balanced in selecting procedures for access to and use of electronic systems, because any increase in security may cause a decrease in convenience. This PKI uses four certificate types in order to permit subscribers and relying parties to select the preferred balance between security and convenience for their intended uses.

The certificate type to be used for any given application, transaction or communication shall be determined by the parties using or engaging in that application, transaction or communication, based upon their judgment as to the appropriate balance between security and convenience for their purposes.

High assurance level certificates are based upon the most secure I&A procedures and strictest subscriber security obligations applicable to this PKI. Basic and rudimentary assurance level certificates are based upon the most convenient I&A procedures and least stringent subscriber security obligations. Medium assurance level certificates fall between high and rudimentary in terms of both convenience and security.

The I&A procedures and subscriber security obligations applicable to each certificate type are described below. Certificates may be issued to persons and electronic devices, subject to the limitations of this policy.

Certificates shall be issued under this policy following I&A of a subscriber's identity in the manner set forth in this policy. A registered CA shall revoke certificates in the circumstances enumerated in section 4.9. A registered CA shall maintain records and information logs in the manner described in sections 5.4 and 5.5.

Private keys shall be created, used and stored in a trustworthy and secure manner. Keys shall have a validity period as indicated in this policy. Confidentiality keys issued by a registered CA shall be backed-up to protect against data loss or data corruption. A registered CA shall not disclose an applicant's or a subscriber's personal information except as provided in this policy. Registered CA activities shall be subject to inspection and/or audit for compliance with this policy in accordance with section 2.7.

1.1.2 General definitions

Terms used herein and in related agreements and other documents incorporating this policy have the following meanings:

Activation data	Private data, but not keys, used or required to access or activate cryptographic modules.
Affiliated person	An individual person who is authorized by an organization to hold a certificate containing the organization's name as an employee, partner, member, officer, agent, licensee, permitee or other associate of the organization.
Applicant	A subscriber, after applying to a registered CA for a certificate, but before the certificate issuance procedure is completed.

Authenticate	To confirm the identity of a person when that identity is presented.
Authenticating RA	A registration authority which, at the request of ITEC as delegated to the CITA, has been authenticated by a registered CA, issued a registration authority certificate by the registered CA, and entered into an agreement with ITEC authorizing the authenticating RA to process subscriber applications for certificates and to conduct I&A of subscribers in accordance with all applicable laws and this policy.
Authority revocation list (ARL)	A list of revoked CA certificates. An ARL is a CRL for registered CA cross-certificates.
Basic assurance level certificate	A certificate issued based upon I&A procedures, which include the applicant's submission of appropriate proof of identity and which may include face-to-face registration by an authenticating RA.
CA certificate	The certificate at the beginning of a certification chain within the State of Kansas PKI hierarchy, which is self-issued in a secure and trustworthy manner.
CA private root key	The private key used to sign the registered CA certificate and certify the registered CA's public/private key pair.
CA private signing key	The private key that corresponds to a registered CA's public key, which is listed in the registered CA certificate and which is used to sign certificates.
Certificate	A computer-based record or electronic message that at a minimum: (i) identifies the registered certification authority issuing it; (ii) names or identifies a subscriber; (iii) contains the public key of the subscriber; (iv) identifies the certificate's operations period; and (v) is digitally signed by a registered certification authority.
Certificate policy (CP)	This policy, which states a named set of rules that indicate the applicability of a certificate to particular communities and classes of applications with common security requirements.
Certificate profile	The protocol stated in section 7 of this policy, which establishes the allowed format and contents of data fields within a certificate.
Certificate revocation list (CRL)	A list maintained by a registered CA of the certificates that it has issued and that are revoked before their stated expiration dates.
Certification authority (CA)	*See* registered CA.
Certification practice statement (CPS)	A statement published by a registered CA that specifies the policies or practices that the registered CA employs in issuing, publishing, suspending and revoking certificates in compliance with this CP.
Chief information technology architect	Also CITA. The Kansas chief information technology architect, acting in accordance with KSA 75-7204. The CITA is the policy management authority (PMA) under this policy.
Chief information technology officer	Also CITO. The Kansas chief information technology officer, one each for the three branches of Kansas government, acting in accordance with KSA 75-7205, 7206 and 7207.

Compliance review	Documentation in the form of an information systems audit report verifying that the applicant has the use of a trustworthy system, as defined in Kansas law.
Confidentiality key	The private key of a key pair used by the subscriber to decrypt messages encrypted with the public key of the key pair.
Cross-certificate	A certificate used to establish a trust relationship between two registered certification authorities.
Cryptomodule	Hardware and/or software that: (i) generates key pairs, (ii) stores cryptographic material and/or (iii) performs cryptographic functions.
Digital signature	A type of electronic signature consisting of a transformation of an electronic message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether: (I) The transformation was created using the private key that corresponds to the signer's public key; and (ii) the initial message has not been altered since the transformation was made.
Distinguished name (DN)	The unique identifier for a subscriber so that the person or device can be located in a directory.
Electronic device	Computer software or hardware or other electronic or automated means configured and enabled by the subscriber to act as its agent and to initiate or respond to electronic records or actions, in whole or in part, without review or intervention by the subscriber.
Globally unique identifier (GUID)	Also called a universally unique identifier (UUID); the result of a process that yields a 24 character long string, containing combinations of numbers, letters and/or special characters and that is appended to the common name (CN) in individual or entity certificates. The GUID may contain only those characters found in the following character set: **ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz 0123456789[ ]-**
Hardware token	A secure hardware device (*e.g.* smartcard or a USB token) used to store a subscriber's private keys and certificates.
High-security zone	An area to which access is controlled through an entry point and limited to authorized, appropriately screened personnel and properly escorted visitors, accessible only from security zones and separated from security zones and operations zones by a perimeter.
Identification and authentication (I&A)	To ascertain and confirm through appropriate inquiry and investigation the identity of a subscriber or other person.
Information network of Kansas	Also INK. The information network of Kansas, acting in accordance with KSA 74-9303.
Information technology advisory board	Also ITAB. The Kansas information technology advisory board.
Information-	Also ITEC. The Kansas information technology executive council, acting in accordance

technology executive council	with KSA 75-7201 *et seq.*
Issue certificates	The acts performed by a registered CA in creating a certificate, listing itself as "issuer," and notifying the authenticating RA or other certificate applicant of its contents and that the certificate is ready and available for acceptance.
Kansas information technology office	Also KITO. The Kansas information technology office.
Key escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer or other party in accordance with provisions set forth in the agreement.
Key generation	The trustworthy process of creating a public/private key pair.
Key pair	Two mathematically related keys having the properties that (i) one key can be used to encrypt a message that only can be decrypted using the other key and (ii) even knowing one key, it is computationally infeasible to discover the other key.
Medium assurance level certificate	A certificate issued based upon I&A procedures, which include face-to-face registration before an authenticating RA and third party identity proofing.
Online certificate status checking protocol (OCSP)	A protocol identified by RFC 2560 that enables an application to determine the status of an identified certificate by issuing a status request to an OCSP responder and suspending acceptance of the certificate in question until the responder has provided the application with a response.
Operations zone	An area where access is limited to personnel who work there and to properly escorted visitors. Operations zones are monitored at least periodically, based on a threat risk assessment and preferably should be entered from a reception zone.
Operative personnel	Operative personnel are individual persons who are agents or employees of an authenticating RA or registered CA.
Out of band	Communication between parties using a means or method that differs from the current method of communication.
Person	Under the Kansas uniform electronic transactions act, an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation or any other legal or commercial entity.
Policy management authority	Also PMA. For this policy, the Kansas chief information technology architect (CITA).
Private key	The key of a public/private key pair kept secret by its holder, used to create digital signatures and to decrypt messages or files that were encrypted with the subscriber's corresponding public key.
Public key	The key of a public/private key pair that is used to verify a digital signature created with

	its corresponding private key, which can be made available publicly in a certificate, and which also can be used to encrypt messages or files which then can be decrypted only with the intended recipient's corresponding private key.
Public key cryptography	A type of cryptography also known as asymmetric cryptography that uses a unique public/private key pair of mathematically related numbers.
Public key infrastructure (PKI)	The architecture, organization, techniques, practices and procedures that collectively support the implementation and operation of a certificate-based public key cryptography system.
Public repository	*See* Repository.
Reception zone	The entry to a facility where the initial contact between the public and a registered CA or authenticating RA occurs, where services are provided, information is exchanged and access to restricted (operations, security and high-security) zones is controlled. To varying degrees, activity in a reception zone is monitored by the personnel who work there, by other personnel or by security staff. Access by the public may be limited to specific times of the day or for specific reasons. Entry beyond the reception zone is indicated by a recognizable perimeter such as a doorway or an arrangement of furniture and dividers in an open office environment.
Registered certification authority	Also registered CA. A person providing certification of a digital signature who is, or is certified by, a member of the group of certification authorities approved by and registered with the secretary of state.
Registration	The process of receiving or obtaining a request for a certificate from a subscriber and collecting and entering the information needed from that subscriber to include in and support I&A and issuance of a certificate.
Registration authorities	*See* authenticating registration authorities.
Relying party	A person who relies on a certificate issued under the terms of this policy.
Relying party agreement	An agreement between a registered CA and any person under which the person has agreed to be bound by all of the provisions of this policy and a registered CA's certification practice statement.
Repository	Also directory. An online system maintained by or on behalf of a registered certification authority for storing and retrieving certificates and other information relating to certificates and digital signatures.
Revocation or revoke a certificate	To prematurely end the operational period of a certificate, effective at a specific date and time.
Rudimentary assurance level certificate	A certificate issued based upon I&A procedures, which include the applicant's application through a network such as the internet, by correspondence or in person.
Secretary	The Kansas secretary of state.
Security zone	An area to which access is limited to authorized personnel and to authorized and properly escorted visitors. Security zones preferably should be accessible from an operations zone through a specific entry point. A security zone is not required to be

	separated from an operations zone by a secure perimeter. A security zone is monitored 24 hours a day and 7 days a week by security staff, other personnel or electronic means.
Shared secret	Activation data used to assist parties in authenticating identity and establishing a reliable channel of communication.
Signature key	The private key of a key pair used by the subscriber for signing and for establishing non-repudiation.
Software cryptomodule	A software program that performs the functions of a cryptomodule.
Sponsoring organization	An organization that has authorized the issuance of a certificate identifying the subscriber as having an affiliation with the organization (*e.g.*, as an employee, partner, member, officer, agent, licensee, permitee or other associate).
State	The State of Kansas.
Strong PIN or password	An alphanumeric code of at least eight characters used to gain access to a locked system.
Subscriber	A person or device who or which is the subject of a certificate, accepts the certificate and holds the private key that corresponds to the public key listed in that certificate.
Third party identity proofing	A process by which an authenticating RA confirms subscriber information provided during registration by verifying it with other organizations and agencies which serve as information or reference services.
Trustworthy system	A secure system that materially satisfies the most recent common criteria protection profile for commercial security, known as "CSPP – guidance for COTS security protection profiles," published by the U.S. department of commerce in December 1999 and hereby adopted by reference. (The previous version of this document was known as "CS2 – protection profile guidance for near-term COTS.")
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage in order to prevent the recovery of the data.

1.1.3 Acronyms

ARL	authority revocation list
CA	certification authority
CITA	chief information technology architect
CITO	chief information technology officer
CMA	certificate manufacturing authority
CP	certificate policy, used interchangeably with "policy"
CPS	certification practice statement

CRL	certificate revocation list
DN	distinguished name
I&A	identification and authentication
INK	information network of Kansas
ITAB	information technology advisory board
ITEC	information technology executive council
KAR	Kansas administrative regulations
KITO	Kansas information technology office
KSA	Kansas statutes annotated
OID	object identifier
OCSP	online certificate status protocol
PKI	public key infrastructure
RA	registration authority
PMA	policy management authority
SOS	secretary of state
X.500	the ITU-T (international telecommunication union-T) standard that establishes a distributed, hierarchical directory protocol organized by country, region, organization, etc.
X.509	the ITU-T (international telecommunication union-T) standard for certificates. X.509, version 3, refers to certificates containing or capable of containing extensions.

1.2 Identification

The American national standards institute (ANSI) has assigned a unique numeric object identifier (OID) of *(to be determined)*. The following OID has been issued to the State of Kansas for this policy: *(to be determined)*, which may not be used except as specifically authorized by this policy.

The policy OID to be asserted in certificates issued in accordance with the policy provisions herein shall have a base arc of: {joint-iso-ccitt (2) country (16) USA (840) organization (1) *(to be determined)* CP (0) State of Kansas (4)}, and all certificates issued under this policy shall reference this arc in the certificate policies field of the certificate.

There are four levels of assurance in this policy, which are defined in subsequent sections. Each level of assurance has an OID to be asserted in certificates issued by the registered CA. The OIDs are identified as follows:

High assurance level certificate
id-highassurancelevel ID::= *(to be determined)*
Medium assurance level certificate
id-mediumassurancelevel ID::= *(to be determined)*
Basic assurance level certificate
id-basicassurancelevel ID::= *(to be determined)*
Rudimentary assurance level certificate
Id-rudimentaryassurancelevel ID::= *(to be determined)*

Each level of certificate shall be issued to certify a key as being used either for signing (digital signature private key) or for encryption (confidentiality key). The use of a specific key shall be determined by the key use extension, discussed in sections 6.1.9 and 7.1.7.

1.3 Community and applicability

This policy describes an open-but-bounded (OBB) public key infrastructure, as described in the internet engineering task force (IETF) public key infrastructure X.509 (PKIX) part 4 framework. A certificate issued in an OBB PKI may be relied upon by multiple parties. A registered CA in an OBB PKI is a legal entity independent of its subscribers and relying parties. A CP adopted for an OBB PKI reflects the agreements and understandings of the parties using the PKI.

The OBB PKI described in this policy is based in the State of Kansas, and this policy shall be interpreted and enforced under the provisions of the Kansas uniform electronic transactions act and the Kansas administrative regulations. Certificates issued pursuant to this policy may be used for communications and transactions and by parties within or outside the State of Kansas, and between parties within and parties outside the State of Kansas.

This policy describes the rights and obligations of persons authorized under this policy to fulfill any of the following roles: certificate service provider roles, end entity roles and policy management authority roles. Certificate service provider roles are registered certification authority, authenticating registration authority, certificate manufacturing authority and repository. End entity roles are subscribers and relying parties. Requirements for persons authorized to fulfill any of these roles are in this section.

The community served by this OBB PKI includes any authorized party (certificate service provider, policy management authority, relying party and subscriber) as defined by this policy.

1.3.1 The policy management authority

The policy management authority (PMA) for this CP has delegated authority from ITEC and advises the ITEC on policy matters.

1.3.1.1 Registration authorities (RAs)

Under this policy, registration authority functions are conducted by authenticating RAs approved by the ITEC as delegated to the PMA, subject to the RA's agreement with the ITEC, including their agreement to comply with all of the applicable provisions of this policy. Only operative personnel of an authenticating RA are authorized to accept applications and conduct I&A.

1.3.1.2 Certificate

A registered CA shall be responsible for the manufacture of certificates. However, a

	manufacturing authorities (CMAs)	registered CA may subcontract functions to third party certificate manufacturing authorities (CMAs) who agree to be bound by all of the provisions of this policy, but a registered CA shall remain responsible for the performance and audit of those services in accordance with this policy.
1.3.2	Repositories	A registered CA shall perform the role and functions of the repository. A registered CA may subcontract performance of the repository functions to a third party repository who agrees to be bound by all of the provisions of this policy, but a registered CA remains responsible for the performance and audit of those services in accordance with this policy.
1.3.3	End entities	
1.3.3.1	Subscribers	A subscriber is the person whose name appears as the subject in a certificate and uses the certificate and corresponding keys in accordance with this policy. A registered CA may issue certificates that reference this policy to persons and electronic devices, provided that responsibility and accountability is attributable to an individual person as custodian of the public/private key pair.
1.3.3.2	Relying parties	A relying party is any person who relies upon a certificate issued under the terms of this policy.
1.3.4	Applicability and applications	
1.3.4.1	Determination of acceptability of certificate type by relying party	This policy does not specify what steps the relying party should take to determine whether to rely upon the certificate. For example, it does not compel the relying party to perform X509 path creation or processing or to determine whether any certificates in the trust path have been revoked. The relying party decides, pursuant to its own or its agency's/ organization's policies, what steps to take; the policy merely provides the tools needed to perform the trust path creation, validation and certificate policy mappings which the relying party may wish to employ in its determination. In addition, this policy contains no limits on the use of any certificates, issued by the registered CA or by authenticating RAs. Instead, persons acting as relying parties shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.
1.3.4.2	Purposes	Certificates that reference this policy are intended to support verification of digital signatures in applications where the identity of communicating parties needs to be authenticated, where a message or file needs to be bound to the identity of its originator by a signature, where the integrity of the file or message has to be assured, to enable encryption for confidential communications and for authentication for access control. The suitability of a given certificate for any given purpose depends upon the level of assurance of the identity of the subscriber required by a relying party for that purpose and the acceptability of digital signatures under applicable law.
1.3.4.3	Prohibited applications	If certificates that reference this policy are proposed to be used by any authority having jurisdiction over an application requiring fail safe performance (such as the operation of nuclear power facilities, air traffic control systems, aircraft navigation systems, weapons control systems or any other system whose failure could lead to injury, death or material environmental damage), the authority having jurisdiction over such application and who proposes such use first shall obtain approval for use of the certificates from the ITEC.

1.3.4.4	Cross-certification	The PMA may approve the issuance of a cross-certificate between registered CAs. Any such cross-certification only shall occur after approval by the PMA and notice to the secretary and all authenticating RAs.

1.4 Contact details

This certificate policy is owned by the State of Kansas ITEC.

1.4.1	Specification / policy administration organization	Communication to the PMA should be addressed to: Director, Kansas Information Technology Office State of Kansas (DISC) Kansas Information Technology Office 900 SW Jackson Topeka, KS 66612
1.4.2	Contact person	Questions regarding the implementation and administration of this policy should be directed to: Director, Kansas Information Technology Office State of Kansas (DISC) Kansas Information Technology Office 900 SW Jackson Topeka, KS 66612
1.4.3	Person determining CPS suitability for policy	The PMA shall determine the suitability of any CPS to this policy.

2 General provisions

Nothing in this policy shall be construed to conflict with, alter or eliminate any other obligation, responsibility or liability that may be imposed on any person by virtue of any contract or obligation that is otherwise determined to be controlling by applicable law.

2.1 Apportioning legal responsibilities among parties

2.1.1 CA obligations, representations and liability

A registered CA shall conduct the following aspects of the issuance and management of certificates:

- acceptance of completed applications and enrollment materials for certificates from authenticating RAs and enrollment of subscribers upon such acceptance;
- the certificate manufacturing process;
- publication, suspension, revocation and renewal of certificates;
- administration of the repository; and
- management of registered CA operations and infrastructure related to certificates in accordance with the requirements, representations and warranties of this policy.

2.1.1.1	Notification of certificate issuance and revocation	A registered CA shall make CRLs available to subscribers and relying parties in accordance with section 4.9. A registered CA shall notify an authenticating RA or, when appropriate, a subscriber when a certificate bearing the subscriber's DN is issued or

revoked.

2.1.1.2 Accuracy of representations

By issuing a certificate that references this policy, a registered CA certifies and warrants to the subscriber and to all relying parties, who reasonably rely on the information contained in the certificate during its operational period and in accordance with this policy, that:

- the registered CA has issued and will manage the certificate in accordance with this policy;
- the registered CA has complied with the requirements of this policy and any applicable CPS when authenticating the subscriber and issuing the certificate;
- there are no misrepresentations of fact in the certificate reasonably known to the registered CA, and the registered CA has taken reasonable steps to verify any additional information in the certificate;
- information provided to the registered CA by the authenticating RA and/or subscriber in the certificate application for inclusion in the certificate has been transcribed accurately to the certificate; and
- the certificate meets all material requirements of this policy and the registered CA's CPS.

2.1.1.3 Time between certificate request and issuance

Certificates shall be issued within the following time period following completion of I&A:

- high assurance level certificates - three (3) business days;
- medium assurance level certificates - three (3) business days;
- basic assurance level certificates - three (3) business days; and
- rudimentary assurance level certificates - three (3) business days.

2.1.1.4 Certificate revocation and renewal

A registered CA shall ensure that any procedures for the expiration, revocation and renewal of a certificate will conform to the relevant provisions of this policy and will be expressly stated in the subscriber agreement and any other applicable document outlining the terms and conditions of the certificate use. A registered CA shall ensure that key changeover procedures are in accordance with section 5.6. A registered CA also shall ensure that notice of revocation of a certificate will be posted to the CRL within the time limits stated in section 4.9. The address of the CRL shall be defined in the certificate.

2.1.1.5 Protection of private keys

A registered CA shall ensure that its private keys and activation data are protected in accordance with parts 4 and 6 of this policy.

2.1.1.6 Restrictions on registered CA's private key use

A registered CA shall ensure that its CA private signing key is used only to sign certificates and CRLs. A registered CA may issue certificates to subscribers, CA and authenticating RA personnel, devices and applications. A registered CA shall ensure that private keys issued to its personnel, employees, officers, agents and subcontractors to access and operate registered CA applications are used only for such purposes.

2.1.1.7 Ensure compliance

A registered CA shall ensure that *only it* accepts and uses registration information

transmitted as follows: (i) directly to the registered CA from subscribers or (ii) directly from an authenticating RA. A registered CA shall ensure that its certification and repository services, issuance and revocation of certificates and issuance of CRLs are in accordance with this policy. Authenticating RAs shall comply with the requirements of this policy when administering any certificates containing this policy's OID or the associated keys. The registered CA and authenticating RAs shall ensure that their authentication and validation procedures are implemented as set forth in part 3.

2.1.1.8 Consequences of breach — *(To be determined.)*

2.1.1.9 Notification of breach — The registered CA shall advise the secretary and the PMA at the earliest possible time of any breach or suspected breach.

2.1.2 Authenticating RA obligations, representations — Under this policy an authenticating RA shall have primary responsibility for all I&A. Authenticating RA functions are considered to be "front-end" functions involving direct contact with certificate applicants and subscribers that leverage the RA's greater knowledge of the certificate applicants and subscribers and its direct relationship to them.

Authenticating RAs shall perform their duties in a manner that is consistent with this policy and that promotes a cooperative relationship with the registered CA. They shall use the keys and certificates issued by the registered CA only for the purposes authorized by this policy and in conformance with the CPS.

The primary obligations of the authenticating RA are:

- the establishment of a trustworthy environment and procedure for certificate applicants to submit their certificate applications (*e.g.* creating a web-based enrollment page);
- the identification and authentication of persons who apply for a certificate;
- the approval or rejection of certificate applications;
- the initiation of certificate revocations, either at the subscriber's request or upon the RA's own initiative; and
- the identification and authentication of persons submitting requests to renew certificates or to obtain a new certificate following a re-keying process and processes set forth above for certificates issued in response to approved renewal or re-keying requests.

2.1.2.1 Notification of certificate issuance and revocation — Unless otherwise provided by law or agreement, there are no requirements that an authenticating RA notify a subscriber or relying party of the issuance or revocation of a certificate.

2.1.2.2 Accuracy of representations — When an authenticating RA submits subscriber information to a registered CA, it shall certify to the registered CA that it has authenticated the identity of that subscriber in accordance with parts 3 and 4 of this policy.

2.1.2.3 Protection of private — Each person performing authenticating RA duties on-line through a remote

	keys	administration application with the registered CA shall ensure that the person's private keys are protected in accordance with parts 5 and 6.
2.1.2.4	Restrictions on private key use	Private keys used by an RA administrator to access and operate RA applications on-line with the registered CA shall not be used for any other purpose.
2.1.2.5	Authenticating RA security and operations manual	Each authenticating RA shall comply with the provisions of the authenticating RA security and operations manual provided to RAs by the PMA.
2.1.2.6	Consequences of breach	*(To be determined.)*
2.1.2.7	Notification of breach	The authenticating RA shall advise the secretary, the PMA and the registered CA at the earliest possible time of any breach or suspected breach.
2.1.3	Subscriber obligations, representations and liability	The responsibilities of each subscriber for a certificate shall be:
2.1.3.1	Representations	Upon application for a certificate and in all subsequent communications, to provide complete and accurate responses to all appropriate requests for information made by the registered CA or authenticating RA during the applicant registration, certificate application and authentication of identity processes; and upon notice to the subscriber of issuance of a certificate naming the applicant as the subscriber, to review the certificate to ensure that all subscriber information included in it is accurate and to accept or reject the certificate in accordance with section 4.4;
2.1.3.2	Subscriber security obligations/ protection of subscriber private key and key token	To generate a key pair using a secure system, and to take appropriate precautions to prevent any compromise, modification, loss, disclosure or unauthorized use of the private key. "Appropriate precautions" and "secure system," for purposes of the different types of certificate provided for in this policy, shall mean the following:
2.1.3.2.1	Rudimentary and basic assurance level certificates	To use reasonable efforts to protect the private key for a rudimentary and basic assurance level certificate, which may be stored in the browser of any computer at the subscriber's election and risk. Use of a password or PIN to protect the private key shall be required.
2.1.3.2.2	Medium assurance level certificates	To use reasonable efforts to protect the private key for a medium assurance level certificate, which shall include storage in a hardware token or software cryptomodule protected by a strong PIN or password.
2.1.3.2.3	High assurance level certificates	To use reasonable efforts to protect the private key for a high assurance level certificate, which shall include storage in a hardware token or software cryptomodule, protected by a strong PIN or password.
2.1.3.3	Restrictions on end-entity private key use	To use the certificate and the corresponding private key exclusively for purposes authorized by this policy and only in a manner consistent with this policy; and

2.1.3.4	Notification upon private key compromise	To instruct the registered CA or authenticating RA to revoke the certificate promptly upon any actual or suspected loss, disclosure, or other compromise of the private key, or, in the case of a certificate issued to an affiliated individual under section 3.1.8, when the affiliated individual no longer is affiliated with the organization.
2.1.3.5	Consequences of breach	A subscriber who is found to have acted in a manner inconsistent with these obligations shall have his, her or its certificate revoked and shall forfeit all claims he, she or it may have against any other party to the PKI in the event of a dispute arising from the failure to fulfill the obligations above.
2.1.4	Relying party obligations, representations and liability	Before using a subscriber's certificate, a relying party shall ensure that it is appropriate for the intended use.
2.1.4.1	Revocation check responsibility	A relying party shall check the status of the certificate through OCSP or against the appropriate and current CRL in accordance with the requirements stated in section 4.9 (as part of this verification process the digital signature of the CRL also shall be validated).
2.2	***Limitation on liability***	No provision.
2.3	***Financial responsibility***	A registered CA shall provide the following financial assurances:
2.3.1	A registered CA	A registered CA shall obtain and maintain a good and sufficient surety bond, certificate of insurance or other evidence of financial security in the amount of $100,000. Pursuant to Kansas law, if the registered CA fails to comply with this provision, the CA's registration with the secretary may be deemed lapsed.
2.4	***Interpretation and enforcement***	
2.4.1	Governing law	The laws of the United States of America and the State of Kansas shall govern the enforceability, construction, interpretation and validity of this policy.
2.4.2	Specific provisions: severability, survival, merger and notice	A registered CA shall ensure that any agreements by that registered CA will contain provisions governing severability, survival, merger or notice consistent with Kansas law.
2.4.3	Dispute resolution procedures	ITEC, with assistance from the PMA, shall resolve any disputes associated with the use of the registered CA or certificates issued by the registered CA.
2.5	***Fees***	Notice of any fee charged to a subscriber or relying party shall be given to that person.
2.5.1	Certificate issuance, renewal, suspension and revocation fees	*(To be determined.)*
2.5.2	Certificate access fees	*(To be determined.)*

2.5.3	Revocation status information access fees (certificate validation services)	*(To be determined.)*
2.5.4	Fees for other services such as policy information	No fee shall be charged for access to review the provisions of this policy.
2.5.5	Refund policy	Any fees collected for certificate applications that are not approved shall be refunded.

2.6 Publication and Repository

2.6.1	Publication of CA information	A registered CA shall operate a secure on-line repository that is available to relying parties and that contains (i) issued certificates that reference this policy, (ii) a certificate revocation list (CRL) or on-line certificate status database, (iii) the registered CA's certificate for its CA private signing key, (iv) past and current versions of the registered CA's CPS, (v) a copy of this policy and (vi) other relevant information relating to certificates that reference this policy.
2.6.2	Frequency of publication	Certificates shall be published following the subscriber acceptance procedure specified in section 4.4. The CRL shall be published as specified in section 4.9.
2.6.3	Access controls	A registered CA shall not impose any access controls on this policy, the registered CA's certificate for its CA private signing key and past and current versions of the registered CA's CPS. A registered CA may impose access controls on certificates and certificate status information in accordance with provisions of this policy.
2.6.4	Location	The location of publication shall be one that is convenient to the certificate-using community and appropriate to the total security requirements. It shall identify an X.500 directory and an LDAP interface.
2.6.5	Revocation information	The sole sources of information regarding the validity or revocation of a certificate shall be that which is provided by an authenticating RA, the registered CA or a repository.

2.7 Compliance reviews

2.7.1	Frequency	A registered CA shall submit to and pay for compliance reviews applicable to registered certification authorities under Kansas law. An applicant CA and a registered CA shall file the review report with the secretary upon initial registration as a certification authority and thereafter once every two years unless ordered as follows. The secretary or the PMA may order a compliance review at any time at their discretion.
2.7.2	Identity and qualifications of auditor	A compliance auditor shall be qualified to conduct a compliance review pursuant to Kansas law and shall be sufficiently familiar with the best practices of a registered CA.
2.7.3	Auditor's neutrality	The auditor(s) and registered CA shall have a contractual relationship for the performance of the review, and the auditor(s) shall be sufficiently separated legally and

		organizationally from the registered CA to provide an arms-length, unbiased, independent evaluation.
2.7.4	Scope of reviews	Reviews shall be conducted in accordance with Kansas law and in accordance with the most current version of "CSPP – guidance for COTS security protection profiles," published by the U.S. department of commerce (most current at this drafting: December 1999).
2.7.5	Communication of results	The results of any reviews of the registered CA shall be reported to the registered CA and filed with the PMA and with the secretary as required by Kansas law.
2.7.6	Actions taken as a result of review	If a review reports any material noncompliance with applicable law, this policy or any other contractual obligations of a registered CA, the registration of the CA may be deemed lapsed in accordance with Kansas law.
2.8	***Privacy and data protection policy***	An authenticating RA and registered CA shall use subscriber information only for the purpose of performing the authentication process and issuing a certificate.
2.8.1	Private key information	Digital signature private keys shall be confidential. Any key information disclosure by a subscriber shall be at the subscriber's own risk. Any private key management keys held by a registered CA shall be confidential. Never shall any private key appear unencrypted outside the cryptographic module.
2.8.2	Registered CA and authenticating RA information	All information stored locally on registered CA and authenticating RA equipment (not in the repository) shall be secured as confidential information, and access to it shall be restricted to those with an official need-to-know in order to perform their official duties with regard to the PKI. Private keys used to sign certificates that will assert security privileges shall be classified at the same level as the privileges that are to be asserted by the related certificates. If a registered CA does not independently verify security privilege information, this requirement shall be executed by the authenticating RAs.
2.8.3	Compliance review information	Compliance review information is confidential and shall not be disclosed to anyone for any purpose except for conduct of the compliance review, reporting obligations pursuant to this policy, the registered CA contract with the secretary, the Kansas UETA and the KARs.
2.8.4	Permitted acquisition of private information; disclosure	A registered CA only shall collect such personal information about a subscriber that is required for the issuance of a certificate to the subscriber. For the purpose of proper administration of certificates, a registered CA or authenticating RA may request non-certificate information to be used in issuing and managing certificates (*e.g.*, identifying numbers, business or home addresses and telephone numbers). Collection of personal information shall be subject to collection, maintenance, retention and protection requirements of applicable state and federal law.
2.8.5	Opportunity of owner to correct private information	Information shall be made available by a registered CA or authenticating RA to the subscriber involved, following an appropriate written request by such subscriber, and shall be subject to correction and/or revision by the subscriber.

2.8.6	Release of information for criminal or civil matter, PMA and secretary roles	Only the PMA or secretary may authorize disclosure of certificate or certificate-related information to a law enforcement agency or other duly-authorized agent in a criminal or civil matter and only under the following circumstances: when (i) required to be disclosed by law, governmental rule or regulation or court order; or (ii) authorized by the subscriber when necessary to effect an appropriate use of the certificate. Any request for such disclosure of private and/or confidential information shall be made in accordance with applicable law.
2.9	***Intellectual property rights***	The private key shall be treated as the sole property of the legitimate holder of the corresponding public key identified in a certificate. This certificate policy and its OID are the property of the ITEC and may be used by an authenticating RA or a registered CA in accordance with the provisions of this policy. Any other use of the above without the express written permission of the ITEC through the PMA is prohibited.
2.10	***Validity of certificates***	
2.10.1	Acceptance	The act of accepting a certificate by a subscriber shall be logged by the registered CA and may consist of a record made when the certificate subject downloads the certificate. Such act shall be recorded and maintained in an auditable trail kept by the authenticating RA or registered CA in a trustworthy manner that complies with industry standards and any applicable laws.
2.10.2	Operational period	Unless accepted or waived by a relying party, after its expiration date an expired certificate no longer shall be used for purposes of authentication, signing and non-repudiation.
2.10.3	Validity of actions during operational period and legal	All relying parties' digital signature verification applications shall be capable of verifying that the digital signature was created during the certificate's operational period.

3 Identification and authentication

3.1	***Initial registration***	The PMA shall establish trustworthy procedures whereby RAs may be authenticated by the registered CA and issued a certificate (collectively, such RAs shall be called "authenticating RAs"). An authenticating RA may designate one or more individuals as its agent(s) to conduct registration activities and authorize them to represent the RA in connection with the issuance and revocation of certificates for subscribers. The registered CA may rely on such designated individual(s) appointed by the authenticating RA to properly authenticate individual applicants. The authenticating RA and its agents shall require proof of identity, as required in this part 3 of the policy.
		Subject to the requirements noted below, certificate applications may be delivered by the applicant to a registered CA or an authenticating RA (and authorizations to issue certificates may be delivered by an authenticating RA to a registered CA) electronically by e-mail or a web site, provided that all communication is secure, *e.g*. by using SSL or a similar security protocol, by first class U.S. mail or in person.
		When an applicant registers his or her information with an authenticating RA or a registered CA and a subscriber account is created, a GUID shall be associated with the subscriber's account. A subscriber's account GUID shall remain the same provided the

		certificate is renewed with the authenticating RA or registered CA as provided in section 3.2 or provided the authenticating RA or registered CA elects to revoke and re-issue a certificate instead of suspension.
3.1.1	Types of names	The subject name used for certificates shall be the subscriber's authenticated common name. Each subscriber shall have a clearly distinguishable and unique X.501 distinguished name (DN) in the certificate subject name field and in accordance with PKIX part 1. Each subscriber may use an alternative name by use of the subject alternate name field, which also shall be in accordance with PKIX Part 1. The DN shall be in the form of a X.501 printable string and shall not be blank.
3.1.2	Need for names to be meaningful	The contents of each certificate subject and issuer name field shall have an association with the authenticated name of the subscriber. With individuals the authenticated common name shall be a combination of first name, surname, and, optionally, initials. The DN also may include an organizational position or role. With other entities the DN shall reflect the authenticated legal name of the subscriber. Where a certificate refers to a role or position, the certificate also shall contain the identity of the person who holds that role or position. A certificate issued for a device or application shall include the authenticated name of the application and/or name of the person or organization responsible for that device or application.
3.1.3	Rules for interpreting various name forms	A registered CA shall defer to a naming authority for guidance on name interpretation and subordination.
3.1.4	Uniqueness of names	The subject name listed in a certificate shall be unambiguous and unique for all certificates issued by a registered CA and shall conform to X.500 standards for name uniqueness. Additional numbers or letters shall be appended to the real name (to ensure the name's uniqueness within the domain of certificates issued by a registered CA) and shall conform to the definition of the GUID stated in this policy. Each name shall be unique and dedicated to a single unique entity.
3.1.5	Name claim dispute resolution procedure	Although a registered CA shall defer to a naming authority, as described in 3.1.3, it ultimately shall exercise sole discretion in determining subscriber names for certificates it issues. If necessary, a party requesting a certificate may be required to demonstrate its right to use a particular name. The registered CA shall investigate, and correct if necessary, any name collisions brought to its attention. A name collision shall be deemed a compromise of the registered CA's security and shall be remedied in accordance with its CPS and this policy.
3.1.6	Recognition, authentication and role of trademarks	No subscriber shall be guaranteed that its name will contain a trademark, trade name, corporate name or other specific referential material, although the authenticating RA and registered CA may attempt to accommodate such requests. The authenticating RA and registered CA shall not knowingly allow an entity to hold a name that a civil court has determined it has no right to use. Neither shall have any obligation to make any inquiry or investigation into the existence or validity of such an order or the status of any trademark and shall not be required to revoke and re-issue such a name to the rightful owner if it already has issued one sufficient for identification within the PKI.

3.1.7	Method to prove possession of private key	Subscribers shall prove possession of the private key corresponding to the public key in a certificate request. For signature keys, this may be accomplished by signing the request. An authenticating RA or registered CA shall confirm that the applicant is in possession of the private key corresponding to the public key that was submitted with the application in accordance with an appropriate secure protocol implemented by the registered CA and approved by the PMA. Before the issuance of a certificate, the subscriber shall confirm its identity using an appropriate secure protocol selected by the authenticating RA or registered CA in consultation with the PMA. For encryption keys, an authenticating RA or a registered CA may encrypt the subscriber's certificate in a confirmation request message. The subscriber then may decrypt and return the certificate to the authenticating RA or registered CA in a confirmation message. Other procedures also may be acceptable. If the private key is generated directly on a hardware token or smart card, or in a key generator that benignly transfers the key to the token or smart card, then the subscriber is deemed to be in possession of the private key at the time of generation or transfer. If the subscriber is not in possession of the token or smart card when the key is generated, then the token or smart card shall be delivered immediately to the subscriber by a trustworthy and accountable method (see section 6.1.2).
3.1.8	I&A procedures for persons that are entities	An authenticating RA shall comply with the procedures prescribed by the PMA for authenticating persons that are entities.
3.1.9	I&A for individual person	An authenticating RA shall ensure that the applicant's identity information is verified in accordance with the procedures prescribed by the PMA for authenticating persons who are individuals. An RA shall ensure that the applicant's identity information and public key are bound satisfactorily. In addition, the authenticating RA shall record in writing the process that was followed for issuance of each certificate. Process information shall depend upon the level of assurance, and documentation of it shall include: ? the identity of the person performing the identification; ? a signed declaration by that person that he or she verified the identity of the subscriber as required by the applicable procedure; ? a unique identifying number from the ID of the verifier and, if in-person identity proofing is conducted, from the ID of the applicant; ? the date and time of the verification; ? a declaration of identity. The declaration shall be signed with a handwritten signature by the certificate applicant; if in-person identity proofing is conducted, this shall be performed in the presence of the person performing the identity authentication. Where the applicant is not a human being but is instead a network device or some other entity, the requirements pertaining to identity proofing shall be conducted through the human owner or designated representative.

3.1.9.1 High assurance level certificates

The applicant shall appear in person before the authenticating RA.

The applicant shall present at least one approved Kansas government-issued official picture identification credential or two non-Kansas government issued official identification credentials, at least one of which must be a photo ID, such as a drivers license. As an alternative to presentation of identification credentials, other methods of equivalent or greater assurance (such as comparison of biometric data to identities pre-verified to the standards of this CP, obtained by authenticated interaction with secured databases) may be used.

When private keys are delivered to subscribers by hardware tokens, the subscriber personally shall appear before the authenticating RA to obtain his or her token or token activation data.

The private key corresponding to the public key offered for the certificate shall exist in a hardware token, and its possession by the applicant shall be proven in accordance with PKIX certificate management protocol or an equivalent protocol defined in the CPS and approved by the PMA. The certificate shall contain an X.500 distinguished name and optional alternative subject name if marked non-critical.

3.1.9.2 Medium assurance level certificates

The applicant shall appear in person before the authenticating RA.

The applicant shall present at least one Kansas government-issued official picture identification credential or two non-Kansas government issued official identification credentials, at least one of which must be a photo ID, such as a drivers license. As an alternative to presentation of identification credentials, other methods of equivalent or greater assurance (such as comparison of biometric data to identities pre-verified to the standards of this CP, obtained by authenticated interaction with secured databases) may be used.

The applicant's identity shall be personally verified by the authenticating RA, or the applicant shall provide credential information which required an antecedent in-person appearance before an entity accepted by the authenticating RA. For example, if the applicant has a credential that was digitally signed by an entity accepted by the authenticating RA and that required the applicant to make an in-person appearance before that entity, that credential may be accepted on-line along with other information without requiring an in-person appearance before the authenticating RA. The certificate shall contain a distinguished name and may contain an alternative subject name marked as non-critical.

When private keys are delivered to subscribers by hardware tokens, the subscriber shall personally appear before the authenticating RA to obtain his or her token or token activation data.

The private key corresponding to the public key offered for the certificate may exist in software or a hardware token, and its possession by the applicant shall be proven in accordance with PKIX certificate management protocol or an equivalent protocol defined in the CPS and approved by the PMA. The certificate shall contain an X.500 distinguished name and optional alternative subject name if marked non-critical.

3.1.9.3 Basic assurance level certificates

The applicant may apply in person or through a network (such as the internet), but if the latter is used, the connections between the applicant and the authenticating RA (for registration) and registered CA (for transport of the public key for certificate

issuance) shall be secured using a protocol that provides for strong encryption for the transferring of information and that is defined in the CPS and approved by the PMA.

The applicant shall provide appropriate proof of identity, and the authenticating RA shall vet the information to confirm identity. This may be accomplished by use of a data base or by attestation by a trusted individual in the same organization who has supervisory responsibility for the applicant.

The private key corresponding to the public key offered for the certificate may exist in software or a hardware token, and its possession by the applicant shall be proven in accordance with PKIX certificate management protocol or an equivalent protocol defined in the CPS and approved by the PMA. The certificate shall contain a non-null subject name and may contain an alternative subject name marked as non-critical.

3.1.9.4 Rudimentary assurance level certificates

The applicant may apply in person or through a network (such as the internet) or by correspondence.

No proofing of the applicant's identity is required.

The private key corresponding to the public key offered for the certificate may exist in any software or hardware form. The certificate shall contain either a non-null subject name or, if a null subject name, it shall contain an alternative subject name that is populated and marked as non-critical. This level is intended only for ensuring data integrity checking.

3.1.9.5 All assurance levels

A certificate request identifying an electronic device as the subject of a certificate may be made by an approved subscriber for whom the electronic device's signature is attributable for the purposes of accountability and responsibility. Identification and authentication of the applicant shall follow this policy's requirements as if the approved subscriber were applying for the certificate on his or her own behalf.

3.2 Certificate renewal, update and routine re-key

3.2.1 Certificate re-key

Within three months before the scheduled expiration of the operational period of a certificate issued following authentication under this policy, a subscriber may request issuance of a new certificate for a new key pair from the authenticating RA or registered CA who issued the original certificate, provided the original certificate has not been suspended or revoked. The subscriber's account GUID shall remain unchanged and the same GUID shall appear in the subsequent certificate. Such a request may be made electronically by a digitally signed message based on the old key pair in the original certificate. Renewal of an affiliated individual shall require verification that the affiliation still exists. Such verification of affiliation shall be identical to that required for a new application.

3.2.2 Certificate renewal

Renewing a certificate means creating a new certificate with the same name and authorizations as the old one, but referencing a new key pair, extended validity period and a new serial number. Like certificate re-keying, the subscriber's account GUID shall remain unchanged and appear in the new certificate. A certificate may be renewed if the public key has not become invalid, the private key has not been compromised and the user name and attributes are correct.

3.2.3 Certificate update

Updating a certificate means creating a new certificate that has a different key, a different serial number and one or more other fields that are different from the old certificate. After the subscriber presents the existing certificate to the authenticating

RA or registered CA with the update request, the updated certificate shall be manufactured using the same GUID as the old certificate.

3.3 Re-key-after revocation Revoked or expired certificates shall not be renewed. Applicants without a valid certificate that references this policy from an authenticating RA or registered CA shall be re-authenticated by an authenticating RA after the applicant files a certificate application, identical to a first-time application, except, if it is determined to revoke instead of suspend, the newly issued certificate shall contain the same GUID as the original certificate.

3.4 Revocation request A certificate revocation request that is submitted electronically may be authenticated on the basis of a digital signature using the certificate's associated key pair. The identity of the person submitting a revocation request in any other manner shall be authenticated in accordance with section 3.1. Revocation requests authenticated on the basis of the certificate's associated key pair always shall be accepted as valid. Other revocation request authentication mechanisms may be used as well, including a request in writing signed by the subscriber and sent by U.S. Postal service first-class mail or equivalent. These authentication procedures shall balance the need to prevent unauthorized revocation requests against the need to revoke certificates quickly.

4 Certificate life cycle operations requirements

4.1 Certificate request This policy identifies the required information and procedures that constitute assurance and support trust in the PKI. The following procedures satisfy the security requirements of this document. The following steps shall be required when applying for a certificate: establish the identity of subject as provided above; obtain a public/private key pair for each certificate required; prove to the registered CA that the public key forms a functioning key pair with the private key held by the user, as provided above; provide a point of contact for verification of any roles or authorizations requested.

4.1.1 Who can request a certificate — An applicant for a certificate shall complete a certificate application in a form prescribed by the authenticating RA or registered CA and enter into a subscriber agreement with the authenticating RA and registered CA. All applications shall be subject to review, approval and acceptance by the authenticating RA and registered CA. The certificate application process may be initiated by the persons identified in section 3.1.

4.1.2 Certificate request process — An applicant for a certificate shall complete a certificate application and provide requested information in a form prescribed by the authenticating RA or registered CA and this policy.

4.1.3 Time to process a certificate request — *See* section 2.1.1.3 above.

4.1.4 Application for cross-certificate — The PMA, in consultation with a registered CA, shall specify procedures to apply for a cross-certificate.

4.2 Certificate application validation No provisions

4.3 Certificate issuance

4.3.1	Applicant notification	Upon successful completion of the subscriber I&A process in accordance with this policy and complete and final approval of the certificate application, the registered CA shall issue the requested certificate, notify the authenticating RA and applicant thereof and make the certificate available to the applicant pursuant to a procedure whereby the certificate is initially delivered to, or available for pickup by, the subscriber only. The registered CA shall not issue a certificate without the consent of the applicant and, if applicable, the applicant's sponsor.
4.3.2	Issuance by registered CA, exception	Except for rudimentary assurance level certificates, an authenticating RA or registered CA shall use an out-of-band notification process linked to the certificate applicant's physical U.S. postal mail address, or equivalent, and deliver the certificate only to the subscriber.
4.3.3	Notification of certificate issuance to subscribers	After successful validation of the certificate application and issuance of the certificate, the registered CA shall notify the authenticating RA and subscriber in a trustworthy and confidential manner that the certificate has been issued.

4.4 Certificate acceptance Acceptance is the action by a subscriber that triggers the subscriber's duties and potential liability and that constitutes acceptance of this policy and the terms of any applicable CPS and agreement incorporating this policy. The registered CA shall define in its CPS a technical or procedural mechanism to explain the subscriber responsibilities defined in section 2.1.3, inform the subscriber of the creation of a certificate and the contents of the certificate and require the subscriber to indicate acceptance of the responsibilities and the certificate. This process will depend on factors such as where key is generated and how certificates are posted, *e.g*. a subscriber may agree to its responsibilities at the same time that it accepts the certificate, or agreeing to its responsibilities may be a precondition for requesting a certificate.

4.4.1	Certificate acceptance by the subscriber	As a condition to issuing the certificate, the subscriber shall submit written acceptance or rejection of the certificate to the authenticating RA or registered CA and acknowledge the subscriber obligations under section 2.1.3. By accepting the certificate, the subscriber warrants that all information and representations made by the subscriber, which are included in the certificate, are true.
4.4.2	Notification of certificate issuance to others	Notification of certificate issuance to others may be accomplished by publication of the certificate in a recognized repository.

4.5	***Certificate use***	The authenticating RA and registered CA assume no responsibility for the use of or reliance upon certificates except as provided under this policy.
4.6	***Routine certificate renewal***	Routine certificate renewal may be performed by automatic renewal or re-certification and shall create a new key pair.
4.7	***Processing a request for a new key***	
4.7.1	Circumstances for request of a new certification	If out-of-band processes (*e.g*. a shared secret) remain in place to authenticate the subscriber requesting new key certification, the authenticating RA and registered CA are not required to re-perform I&A of the subscriber.
4.7.2	Who can request certification of a new key	Only the authenticating RA or subscriber may request certification of a new key.
4.7.3	Treatment of a request for certification of a new key	Complete re-authentication of a subscriber by performing the I&A identified in section 3.1 is not required if out-of-band processes remain in place to authenticate the requester, including, for example, the use of a shared secret or bio-metric means of identity verification.
4.7.4	Notification of certification request for a new key to subscriber	The notification procedures used by the authenticating RA or registered CA shall be identical to procedures for a new subscriber request.
4.8	***Certificate modifications***	No provision.
4.9	***Certificate revocation***	
4.9.1	Circumstances for revocation, permissive revocation	An authenticating RA or subscriber may request revocation of a certificate at any time for any reason. A sponsoring organization may request revocation of an affiliated individual certificate at any time for any reason. A registered CA also may revoke a certificate upon failure of the subscriber or any sponsoring organization to meet its obligations under this policy, the applicable CPS, or any other agreement, regulation or law applicable to the certificate. This includes revoking a certificate when a suspected or known compromise of the private key has occurred. If the failure is that of an authenticating RA or sponsoring organization, the registered CA first shall notify the PMA of its proposed action.
	Required revocation	An authenticating RA, subscriber, or a sponsoring organization promptly shall request revocation of a certificate: when the name on the certificate no longer is current, complete or true; when the private key, or the medium holding the private key, associated with the certificate is known to be or suspected to be lost, disclosed, compromised or subjected to unauthorized use in any way; or, when an affiliated individual no longer is affiliated with an authenticating RA or sponsoring organization. A registered CA shall revoke a certificate: upon request of the authenticating RA, subscriber or sponsoring organization; upon failure of the subscriber or the sponsoring organization to meet its material obligations under this policy, any applicable CPS, or

		any other agreement, regulation or law applicable to the certificate; if knowledge or reasonable suspicion of compromise is obtained; if the registered CA determines that the certificate was not properly issued in accordance with this policy and/or any applicable CPS. If the failure is that of an authenticating RA or sponsoring organization, the registered CA first shall notify the PMA of its proposed action.
4.9.2	Who can request revocation	A registered CA summarily may revoke certificates within its domain, provided that notice and cause are given. An authenticating RA may request the revocation of a subscriber's certificate on behalf of the subscriber, the subscriber's sponsoring organization or other authorized party. The subscriber is authorized to request the revocation of his or her own certificate, as is the subscriber's sponsoring organization.
4.9.3	Procedure for revocation request	A certificate revocation request shall be communicated promptly to the registered CA, either directly or through the authenticating RA authorized by ITEC to accept such notices. A certificate revocation request may be communicated electronically if it is digitally signed with the private key of the subscriber or the sponsoring organization. Alternatively, the subscriber or sponsoring organization may request revocation by contacting the authenticating RA or the registered CA in person and providing adequate proof of identification in accordance with this policy or an equivalent method.
4.9.3.1	Revocation request grace period	A registered CA shall revoke a certificate as quickly as practical upon receipt of a proper revocation request and always shall revoke certificates within the time periods described in this section 4.9. Notwithstanding the foregoing, there shall be a grace period of three (3) hours between the time a subscriber makes a revocation request and the time a certificate is revoked.
4.9.3.2	Suspension	A certificate may be suspended following an unsigned request for certificate revocation, pending authentication of the revocation request.
4.9.4	Time to process a revocation request	Promptly following revocation of a certificate, the CRL or certificate status database in the repository, as applicable, shall be updated. All revocation requests and the resulting actions taken by the registered CA shall be archived. Certificates may be revoked prior to their expiration. Revocation is accomplished by notation or inclusion in a set of revoked certificates or other directory or database of revoked certificates.
4.9.5	Certificate revocation lists	
4.9.5.1	CRL issuance frequency	In order to ensure timeliness of information, CRLs shall be issued daily, even if there are no changes or updates to be made. CRLs may be issued more frequently than required; if there are circumstances for which the registered CA will post early updates, the circumstances shall be described with specificity in the CPS. The registered CA shall ensure that superceded CRLs are removed from the directory system upon posting of the latest CRL. If a CRL is issued as a result of a key compromise or revocation, the CRL shall be posted as quickly as feasible, but in any event shall be posted no later than six hours after notification of the compromise or decision to revoke by the registered CA. CAs shall make public the details of certificate revocation information posting, including an explanation of the consequences of using dated revocation information. This information shall be given to subscribers during certificate request or issuance and shall be readily available to relying parties.
4.9.5.2	CRL latency	Interim CRLs shall be made available to relying parties.
4.9.6	On-line	When an on-line certificate status database is used as an alternative to a CRL, such

	revocation/status checking	database shall be updated and checked in accordance with the same requirements as defined for a CRL.
4.9.6.1	Online revocation/status checking availability	Registered CAs shall validate online, near real time the status of the certificate identified in a certificate validation request message.
4.9.6.2	Online revocation checking requirements	Each relying party shall validate every certificate it receives in connection with a transaction in accordance with and by the means identified in the certificate. If it becomes infeasible to obtain revocation information, then the relying party either shall reject use of the certificate or make an informed decision to accept the risk, responsibility and consequences for using a certificate for which authenticity cannot be guaranteed to the standards of this policy.
4.9.6.3	Other forms of revocation advertisements available	A registered CA also may use other methods to publicize revoked certificates.
4.10	***Certificate status services***	See 4.9.6
4.11	End of subscription	If a person's subscription to the PKI ends prior to the expiration of any certificates issued under that subscription, the registered CA shall revoke any certificates issued or held under the subscription.
4.12	Private key recovery	A private signing key never shall be stored for purposes of recovery by a CA. If a key pair is used for both signature and confidentiality purposes, recovery of the private key is prohibited.

5 CA facility and management controls

5.1 Physical controls

A registered CA, and all authenticating RAs, CMAs and repositories, shall implement appropriate physical security controls to restrict access to the hardware and software (including the server, workstations and any external cryptographic hardware modules or tokens) used in connection with providing CA services. Access to such hardware and software shall be limited to those personnel performing in a trusted role, as described in the section on procedural controls (5.2.1). Access shall be controlled through the use of electronic access controls, mechanical combination locksets or deadbolts. At all times, such access controls shall be monitored manually or electronically for unauthorized intrusion.

5.1.1 Site location and construction

Any registered CA site shall:

- satisfy the requirements for a security zone;
- be monitored manually or electronically for unauthorized intrusion at all times;
- ensure that access to the registered CA server is limited to those personnel identified on an access list and implement dual access control requirements to the registered CA server for such personnel;

- ensure personnel not on the access list are properly escorted and supervised;
- ensure a site access log is maintained and inspected periodically; and
- ensure all removable media and paper containing sensitive plain text information are stored in containers either listed in or of equivalent strength as those listed in the security equipment guide.
- additionally, the location of the registered CA server shall satisfy the requirements for a high-security zone.

All authenticating RA sites shall be located in areas that satisfy the controls required for a reception zone. If an authenticating RA workstation is used for on-line entity management with the registered CA, the workstation shall be located in either:

- a security zone; or
- an operations zone while attended, with all media securely protected when unattended.

If the authenticating RA has possession of a cryptographic module, system software and private keys, then the ITEC through the PMA shall ensure that the operation of the authenticating RA's site provides appropriate security protection for them. The PMA shall conduct a threat and risk assessment of any such site. Security shall include but may not be limited to:

- storage of the cryptographic module and the authenticating RA administrator's private key in a secure container or safe.
- recording of PINs or passwords only in security containers accessible only to designated personnel.
- employees of authenticating RAs shall not leave their workstations unattended when the cryptography is in an unlocked state (*e.g.*, when the PIN or password has been entered).
- a workstation that contains private keys on a hard drive shall be physically secured or protected with an appropriate access control product.
- hardware cryptomodules shall be protected physically, which may be accomplished with site protection.

5.1.2 Physical access

CA equipment always shall be protected from unauthorized access. Authenticating RA equipment shall be protected from unauthorized access while the cryptomodule is installed and activated. The authenticating RA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptomodule is not installed and activated. These security procedures shall be commensurate with the level of threat in the authenticating RA equipment environment. For example, authenticating RA equipment in facilities with controlled access that is occupied primarily by security personnel will not require an additional layer of controlled access surrounding inactivated authenticating RA equipment. Authenticating RA equipment in less secure environments will require additional protection, *e.g.* location in a room that is kept locked when the authenticating RA is not present. Removable CA cryptomodules shall be inactivated and placed in locked containers that will provide security commensurate

with the classification, sensitivity or value of the information being protected by the certificates issued. Any activation information used to access or enable the cryptomodule or CA equipment shall be stored separately. Such information shall be memorized.

A security check covering the facility that houses CA equipment shall occur at least once every 24 hours. The check shall ensure that: the equipment's status is appropriate to the current mode of operation (*e.g.*, that cryptomodules and removable hard disks are in place when "open", and secured when "closed"); any security containers are properly secured; physical security systems (*e.g.*, door locks, vent covers) are functioning properly; and the area is secured against unauthorized access. A specifically identified role or person shall be responsible for making such checks. When a role is responsible, a log identifying the individual performing such a check shall be maintained. A record shall be kept that describes the types of checks performed, the time and the person who performed them. If the CA equipment is located in a continuously attended facility, there shall be a security check of the facility at least once per shift. If the facility is not continuously attended, the last person to leave the facility shall initial a sign-out sheet that states that the facility entrance door is locked and that, where installed, intrusion detection systems are activated. If the facility housing the CA equipment will be unattended for periods greater than 24 hours, it shall be protected by an intrusion detection system. Additionally, a check shall be made at least once every 24 hours to ensure that all doors to the facility are locked and that there have been no attempts by unauthorized persons to enter.

5.1.3 Power and air conditioning

The facility, which houses registered CA equipment, shall be supplied with power and air conditioning sufficient to create a reliable operating environment. In addition, personnel areas within the facility shall be supplied with sufficient utilities to satisfy operational, health and safety needs. The actual quantity and quality of utility service will depend on how the facility operates, *e.g.*, its times of operation (24 hours/7 days or 8 hours/5 days) and whether on-line certificate status checking is provided. The registered CA equipment shall have backup capability sufficient to automatically lockout input, finish any pending actions and record the state of the equipment before lack of power or air conditioning causes a shutdown. Users who require extended operation hours or short response times may contract with the registered CA for additional requirements for backup power generation. The revocation operations shall be supported by uninterruptible power supplies and sufficient backup power generation.

5.1.4 Water exposure

This policy makes no provision for prevention of exposure of CA equipment to water beyond that called for by best business practice. Registered CA equipment shall be installed so that it is not in danger of exposure to water, *e.g.*, placement on tables or elevated floors. Moisture detectors shall be installed in areas susceptible to flooding. Registered CA operators who have sprinklers for fire control shall have a contingency plan for recovery should the sprinklers malfunction or cause water damage outside of the fire area.

5.1.5 Fire prevention and protection

This policy makes no provision for prevention of exposure of registered CA equipment to fire beyond that called for by best business practice. An automatic fire extinguishing system shall be installed in accordance with local code.
A registered CA shall have a contingency plan, which contemplates and addresses damage by fire.

5.1.6 Media storage

Media shall be stored in a manner that protects it from accidental damage (water, fire, electromagnetic). Media that contains audit, archive or backup information shall be stored in a location separate from the registered CA equipment.

5.1.7	Waste disposal	Normal office waste shall be removed or destroyed in accordance with best business practices. Before disposal, media used to collect or transmit information discussed in section 2.8 shall be destroyed in such a manner that the information is unrecoverable.
5.1.8	Off-site backup	System backups, sufficient to provide recovery from system failure, shall be made on a periodic schedule, which shall be described in the CPS. At least one backup copy shall be stored at an offsite location (separate from the registered CA equipment). Only the latest backup is required to be retained. The backup shall be stored at a site with physical and procedural controls commensurate with that of the operational registered CA system.
5.2	***Procedural controls***	
5.2.1	Trusted roles	A trusted role is one whose incumbent performs functions that may introduce security problems if not carried out properly, whether accidentally or maliciously. The individual persons selected to fill these roles shall be above reproach and shall perform their duties carefully, as described in the next section. The duties performed in these roles form the basis of trust in the entire PKI. Two approaches shall be taken to increase the likelihood that these roles may be successfully performed. The first approach is to design and configure the technology to avoid mistakes and prohibit inappropriate behavior. The second is to distribute the functions among several persons, so that any prohibited activity requires collusion. The primary trusted roles defined by this policy are the authenticating RA and the registered CA. Other trusted roles may be defined in other documents, which describe or impose requirements on the registered CA's operation.
5.2.1.1	Registered certification authority (CA)	All certificates referencing this policy shall be issued by CA facilities operating under the direct control of a registered CA. The responsible person or persons identified as operating the registered CA facilities shall be named and made available during compliance audits. Any registered CA who has been assigned a policy identifier defined in this document is subject to the stipulations of this policy. A registered CA's role and the corresponding procedures a registered CA will follow shall be defined in detail in a certification practices statement (CPS) and, perhaps, also in a concept of operations and procedural handbook (CONOP). A registered CA's primary responsibilities shall be to ensure that the following functions occur according to the provisions of this policy: certificate generation and revocation; posting certificates and CRLs; performing the daily incremental database backups; administrative functions such as compromise reporting and maintaining the database; hardware cryptomodule programming and management.
5.2.1.2	Registration authority (RA)	Any authenticating RA that operates under this policy shall be subject to the provisions of this policy and of the registration authority agreement it has with ITEC. An authenticating RA's primary responsibilities shall be: establishing a trustworthy environment and procedure for certificate applicants to submit their certificate applications (*e.g*. creating a web-based enrollment page); identifying and authenticating persons who apply for a certificate; approving or rejecting certificate applications; initiating certificate revocations, either at the subscriber's request or upon the authenticating RA's or sponsor organization's initiative; and identifying and authenticating persons submitting requests to renew certificates or seeking a new certificate following a re-keying process and processes set forth in this policy for certificates issued in response to approved renewal or re-keying requests. *See* 2.1.2.

The responsibilities and controls for authenticating RAs shall be specifically described in a registration authority agreement with ITEC.

5.2.2 Number of persons required per task

A registered CA shall use commercially reasonable practices to ensure that one person acting alone cannot compromise security.

To ensure that one person acting alone cannot compromise security, responsibilities at the registered CA server shall be shared by multiple roles and persons. Each account on the registered CA server shall have capabilities limited to and commensurate with the role of the account holder.

A registered CA shall ensure that no single person may gain access to subscriber private keys stored by the registered CA. At a minimum, procedural or operational procedures shall be in place to perform a key recovery, preferably using a split-knowledge technique, such as two persons each with a separate password, to prevent the disclosure of the encryption key to an unauthorized person. Multi-user control also is required for registered CA key generation, as outlined in 6.2.2. All other duties associated with registered CA roles may be performed by an individual person operating alone. A registered CA shall ensure that any verification process it employs provides for oversight of all activities performed by privileged registered CA role holders.

To ensure the integrity of registered CA equipment and operation, a separate individual shall be identified for each trusted role. The separation provides a set of checks and balances on the registered CA operation. Never shall the incumbent of a registered CA role perform its own auditor function.

5.2.3 Identification and authentication for each role

All registered CA personnel shall have their identity and authorization verified before they are: included in the access list for the registered CA site, included in the access list for physical access to the registered CA system, given a certificate for the performance of their registered CA roles and given an account on the PKI system. Each of these certificates and accounts (with the exception of registered CA signing certificates) shall: be directly attributable to a person, not be shared and be restricted to actions authorized for that role through the use of registered CA software, operating system and procedural controls. Registered CA operations shall be secured using methods such as token-based strong authentication and encryption when the operations are accessed across a shared network.

5.3 Personnel controls

5.3.1 Background qualifications experience and clearance requirements

Registered CAs, authenticating RAs, CMAs and repositories shall implement and follow personnel and management policies sufficient to ensure the trustworthiness and competence of their employees and of the satisfactory performance of their duties in manner consistent with this policy. These policies shall include the certification of all appropriate personnel as “operative personnel.”

5.3.2 Background check procedures

Registered CAs shall cooperate with and pay for an appropriate background check of all personnel who serve in trusted roles (prior to their employment and periodically thereafter as necessary) to verify their trustworthiness and competence in accordance with the requirements of this policy and registered CA's personnel practices, or equivalent. All personnel who fail an initial or periodic background check shall not serve or continue to serve in a trusted role. Background check procedures shall be described in the CPS. They shall be or shall be equivalent to a *category 2* background check, as conducted by the Kansas bureau of investigation, and, if equivalent, as

		approved by the PMA and the secretary. Before conduct of the background check, the person who is subject of the background shall fully respond in writing to the inquiries on a background disclosure form provided by the PMA or secretary. The PMA or the secretary may request conduct of periodic background checks or update of background checks at their discretion.
5.3.3	Training requirements	A registered CA shall ensure that all personnel performing duties consistent with the duties of operative personnel for a registered CA shall receive: comprehensive training in the registered CA security principles and mechanisms, security awareness, all PKI software versions in use on the registered CA system, all PKI duties they are expected to perform and disaster recovery and business continuity procedures. ITEC through the PMA shall provide like training in RA systems for the operative personnel of its approved authenticating RAs.
5.3.4	Retraining frequency and requirements	The requirements of 5.3.3 shall be updated periodically to accommodate changes in a registered CA system. Refresher training shall be conducted as required, and a registered CA shall review these requirements at least once a year.
5.3.5	Job rotation frequency and sequence	This policy makes no provision regarding frequency or sequence of job rotation. Local policies, which do impose requirements, shall provide for continuity and integrity of the PKI service
5.3.6	Sanctions for unauthorized actions	In the event of actual or suspected unauthorized action by a person who performs duties with respect to the operation of a registered CA or authenticating RA, a registered CA or, in the case of a person who performs duties for an RA, the authenticating RA shall suspend his or her access to the registered CA and RA systems.
5.3.7	Contracting personnel requirements	A registered CA shall ensure that contractor access to the registered CA site is conducted in accordance with 5.1.1.
5.3.8	Documentation supplied to personnel	Documentation sufficient to define duties and procedures for each role shall be provided to the personnel assigned to that role.
5.4	***Security audit procedures***	
5.4.1	Types of event recorded	Registered CA equipment shall be capable of recording events related to the server (installation, modification, accesses), and the application (requests, responses, actions, publications, and error conditions). Events may be attributable to human action (in any role) or automatically invoked by the equipment. At a minimum, the information recorded shall include the type of event and the time the event occurred. In addition, for some types of events, the success or failure, the source and destination of a message or the disposition of a created object (*e.g.*, a filename) also shall be recorded. When possible, the audit data shall be collected automatically; when this is not possible, a logbook, paper form or other physical medium shall be used. The auditing capabilities of the underlying equipment operating system shall be enabled during installation. A record of file manipulation and account management shall be maintained. These events also shall be recorded during normal operation of the registered CA equipment.
5.4.2	Frequency of processing log	A registered CA shall ensure that its audit logs are reviewed by registered CA personnel at least weekly and that all significant events are explained in an audit log

summary. Such reviews involve verifying that the log has not been tampered with and, then, briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities recorded in the logs. Supporting manual and electronic logs from the registered CA and authenticating RA shall be compared when any action is deemed suspicious. Actions taken following these reviews shall be documented.

5.4.3	Retention period for audit log	The information generated on registered CA equipment shall be maintained on the registered CA equipment until the information is moved to an appropriate archive facility. Deletion of the audit log from the registered CA equipment shall be performed by a person different from the CA operator. This person shall be identified in the registered CA's CPS. Audit logs shall be retained as archive records in accordance with section 5.5.2.
5.4.4	Protection of audit log	The audit log, to the extent possible, shall not be open for reading or modification by any person or by any automated process other than those that perform audit processing. Any person who does not have modification access to the audit log may archive it (note that deletion requires modification access). Weekly audit data shall be moved to a safe, secure storage location separate from the registered CA equipment.
5.4.5	Audit log backup procedures	Audit logs and audit summaries shall be backed up or copied if in manual form.
5.4.6	Audit collection system (internal vs external)	There is no requirement for the audit log collection system to be external to registered CA equipment. The audit process shall run independently and shall not in any way be controlled by the registered CA operator. Audit processes shall be invoked at system startup and cease only at system shutdown. Should it become apparent that an automated audit system has failed, the registered CA operation shall cease until the audit function can be restored. If it is unacceptable to cease registered CA operation, other procedures, which have been arranged previously with the registered CA's auditor, shall be employed to provide the audit function.
5.4.7	Notification to event-causing subject	When an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device or application that caused the event.
5.4.8	Vulnerability assessments	Events in the audit process are logged, in part, to monitor system vulnerabilities. The registered CA shall ensure that a vulnerability assessment is performed, reviewed and revised following an examination of these monitored events.

5.5 Records archival

5.5.1	Types of event recorded	Registered CA archive records shall be sufficiently detailed to establish the proper operation of the registered CA or the validity of any certificate (including those revoked or expired) issued by the registered CA. At a minimum, the following data shall be recorded for archive for all assurance levels: registered CA accreditation (if applicable) certification practice statement contractual obligations system and equipment configuration modifications and updates to system or configuration

certificate requests
revocation requests
subscriber identity authentication data as stated in section 3.1
documentation of receipt and acceptance of certificates
documentation of receipt of tokens
registered CA re-key
all CRLs issued and/or published
all audit logs
other data or applications to verify archive contents
documentation required by compliance auditors

5.5.2 Retention period for archive

A registered CA shall maintain documentation of compliance with the provisions of this policy, the Kansas uniform electronic transactions act, article 41 of the Kansas administrative regulations and any related agreements for a period of not fewer than 10 years.

If the original medium cannot retain the archived data for the required retention period, the registered CA shall transfer the data to a new medium approved by the PMA. Applications required to process the archived data also shall be maintained for the retention period. Before the end of the archive retention period, the registered CA shall provide the archived data and the applications necessary to read the data to a PMA approved archival facility, which shall retain the applications necessary to read the archived data.

A registered CA that discontinues providing certification authority services without making other arrangements for the preservation of the CA's records shall notify the secretary and the subscribers, in writing, of its discontinuance of business, and perform either of the following: (i) revoke all valid certificates and return all records concerning them to the appropriate subscriber; or (ii) submit the records to another registered certification authority or authorities as ordered by the secretary.

5.5.3 Protection of archive

No unauthorized user shall be permitted to write to, modify or delete the archive. For the registered CA, archived records may be moved to another medium when authorized by the PMA. The contents of the archive shall not be released except as determined by the PMA or as required by law. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. Archive media shall be stored in at least two safe, secure storage facilities separate from the registered CA.

The registered CA shall secure its records pursuant to standards that are commercially reasonable within the industry. The records shall be indexed, stored, preserved and reproduced so that they are accurate, complete and accessible to an auditor. They shall be in the English language.

5.5.4 Archive backup procedures

See 5.5.3.

5.5.5 Requirements for time-stamping of records

All records shall be time-stamped.

5.5.6 Procedures to obtain and verify archive information

During any reviews required by this policy, the auditor shall verify the integrity of the archives. Procedures detailing how to create, verify, package, transmit and store the archive information shall be published in the registered CA's CPS.

5.6 Key changeover

A registered CA uses a signature (private) key for creating subscriber certificates; however, relying parties employ the CA certificate (containing the CA's public key) for the life of the subscriber certificate. Therefore, a registered CA shall not issue subscriber certificates that extend beyond the expiration dates of the respective CA certificates; in addition, the CA certificate validity period shall extend one user certificate validity period past the last use of the registered CA private key.

To minimize risk from compromise of a registered CA's private signing key, that key shall be changed more frequently, and only the new key shall be used for certificate signing purposes from that time. The older, but still valid, certificate shall be available to verify old signatures until all of the certificates signed under it also have expired. If the old private key is used to sign CRLs that contain certificates signed with that key, then the old key shall be retained and protected.

The following list summarizes the maximum validity period of the registered CA's signature certificate and the maximum lifetime of the associated authority-signing key (used for certificate signature), separated by a slash. If a CA certificate and key lifetime are selected that are shorter than a subscriber's, then the authenticating RA certificate and key lifetime shall be no longer than that of the registered CA. Note that signature keys that have expired for the purposes of certificate signature still may be used for CRL signature. All values are in years:

Rudimentary and basic assurance level certificates – 10/5
Medium assurance level certificate -- 6/3
High assurance level certificate -- 6/3

5.7 Compromise and disaster recovery

5.7.1 Computing resources software and/or data are corrupted

A registered CA shall establish an appropriate disaster recovery and business resumption plan. The plan shall set up and render operational a facility that is located in a different geographic area and that is capable of providing registered CA services in accordance with this policy within forty-eight (48) hours of an unanticipated emergency. Such plan shall include a complete and periodic test of readiness for such facility. Such plan shall be detailed in the CPS or other appropriate documentation and shall be readily available to relying parties for inspection.

5.7.2 Secure facility after a natural or other type of disaster

A registered CA shall establish a disaster recovery plan outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster. Where a repository is not under the control of the registered CA, the registered CA shall ensure that any agreement with the repository provides that a disaster recovery plan shall be established and documented by the repository.

5.7.3 Entity public key Is revoked

In the event a registered CA's digital signature certificate must be revoked, the registered CA immediately shall notify: ITEC, the PMA, the secretary, all registered CAs to whom it has issued cross-certificates, all of the authenticating RAs, all subscribers and all individuals or organizations who are responsible for a certificate used by a device or application. The registered CA also: shall publish the certificate serial number on an appropriate CRL and revoke all cross-certificates signed with the revoked digital signature certificate. After addressing the factors that led to revocation,

the registered CA may: generate a new registered CA signing key pair and re-issue certificates to all entities and ensure that all CRLs and ARLs are signed using the new key. In the event the revocation of any other entity's digital signature certificate is required, *see* section 4.9.

5.7.4 Entity private key is compromised

In the event of the compromise, or suspected compromise, of a registered CA signing key, the registered CA immediately shall notify all registered CAs with whom it has cross-certified. In the event of the compromise, or suspected compromise, of any other entity's signing key, an entity shall notify the registered CA immediately. The registered CA shall ensure that its CPS or a publicly available document and appropriate agreements contain provisions outlining the procedures it will use to provide notice of compromise or suspected compromise. In the event of the compromise of a registered CA's digital signature key, the registered CA shall revoke all certificates issued using that key and provide appropriate notice (see 5.7.3). After addressing the factors that led to key compromise, the registered CA may: generate a new registered CA signing key pair; re-issue certificates to all entities and ensure that all CRLs and ARLs are signed using the new key.

5.7.5 Entity public key Is downgraded

In the event the downgrade of a registered CA's digital signature certificate is required, a registered CA immediately shall notify all interested parties including the PMA, other CAs with whom it cross-certified, all authenticating RAs and all subscribers.

5.8 CA termination

A registered CA that discontinues providing certification authority services without making other arrangements for the preservation of the CA's records shall notify the secretary and the subscribers, in writing, of its discontinuance of business, and perform either of the following: (i) revoke all valid certificates and return all records concerning them to the appropriate subscriber; or (ii) submit the records to another registered certification authority or authorities as ordered by the secretary.

5.9 Customer service

A registered CA shall implement and maintain a customer service center to provide assistance and services to subscribers and relying parties, consistent with this policy. The service shall include a system for receiving, recording, responding to, and reporting problems within its own organization and for reporting such problems to the PMA and the secretary.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key pairs for registered CAs, CMAs, authenticating RAs, repositories and subscribers shall be generated so that the private key only is known by the authorized user of the key pair. Acceptable ways of accomplishing this include having all users (CAs, CMAs, authenticating RAs, repositories, and subscribers) generate their own keys on a secure system (and not reveal the private keys to anyone else) and by having keys generated in hardware tokens from which the private key cannot be extracted. Registered CA, authenticating RA and CMA keys shall be generated in hardware tokens. Key pairs for repositories, and end-entities may be generated in either hardware or software.

6.1.2 Private key delivery to entity

In most cases, a private key will be generated and remain within the crypto boundary of the cryptomodule. If the owner of the module generates the key, then there is no

		requirement to deliver the private key. If a key is not generated by the subscriber, then the module shall be securely delivered. Accountability for the location and state of the module shall be maintained until delivery of possession. The subscriber formally shall acknowledge receipt of the module. If the subscriber generates the key and the key will be stored by and used by the application which generated it, or if it is delivered on a hardware token in the possession of the subscriber, no further action is required. If the key must be extracted for use by other applications or in other locations, a protected data structure (such as defined in PKCS#12) shall be used. The resulting file may be kept on a magnetic medium or transported electronically.
6.1.3	Public key delivery to certificate issuer	Public keys shall be delivered to a registered CA in a secure and trustworthy manner, such as a certificate request message. It also may be accomplished by non-electronic means. These means may include, but are not limited to, floppy disk (or other storage medium) sent by registered mail or courier, or by delivery of a token to the registered CA for local key generation at the point of certificate issuance or request. Off-line methods shall include identity checking and shall not inhibit proof of possession of corresponding private key. Any other methods used for public key delivery shall be detailed in a CPS. In those cases where public/private key pairs are generated by the registered CA on behalf of the subscriber, the registered CA shall implement secure procedures to ensure that the token on which the public/private key pair is held is securely sent to the proper subscriber and that the token is not activated prior to receipt by the proper subscriber.
6.1.4	CA public key delivery to users	The public key of a registered CA's signing key pair may be delivered to subscribers in an on-line transaction in accordance with IETF PKIX part 3, or by another appropriate procedure.
6.1.5	Key sizes	Minimum key length for high assurance level certificates is 1024 bits. Minimum key length for rudimentary assurance level certificates is 512.
6.1.6	Public key parameters generation	The digital signature standard shall require key parameters in accordance with FIPS 186. ECDSA shall be used in accordance with draft ANSI standard X9.62.
6.1.7	Parameter quality checking	Parameters for the digital signature standard shall be as specified in FIPS186.
6.1.8	Hardware/software key generation	The generation of digital signature keys for all entities shall be generated randomly in a hardware cryptographic module. Any pseudo-random numbers used for key generation material shall be generated by a FIPS approved method.
6.1.9	Key use purposes (as per X.509 v3 key use field)	Keys may be used for authentication, non-repudiation and message integrity. They also may be used for session key establishment. Registered CA signing keys are the only keys that shall be used for signing certificates and CRLs. The certificate key use field shall be used in accordance with PKIX-1 certificate and CRL profile. One of the following key use values must be present in all certificates: digital signature or non-repudiation. One of the following additional values must be present in registered CA certificate-signing certificates: Key cert sign or CRL sign. Keys shall be certified for use in signing or encrypting, but not both, unless otherwise provided herein. The use of a specific key is determined by the key use extension in the X.509 certificate. This restriction does not prohibit use of protocols (like the secure sockets layer) that provide authenticated connections using key management certificates.

6.2	***CA private key protection***	A registered CA (and the authenticating RA, CMA and repository) each shall protect its private key(s) in accordance with the provisions of this policy.
6.2.1	Standards for cryptographic module	The applicable standard for cryptomodules shall be FIPS140-1 level 2, unless ITEC, with the assistance of the PMA, determines that other comparable validation, certification, or verification standards shall be sufficient. In such event such standards will be transmitted to registered CA's by PMA and published by the registered CA's. Subscribers shall use cryptographic modules, which at a minimum meet the criteria specified in this policy. Authenticating RAs shall have at least level 2 hardware cryptomodules. A higher level may be used if available or desired. Authenticating RAs and registered CAs shall provide the option of using any acceptable cryptomodule, to facilitate the management of certificates. A registered CA may use hardware or software cryptomodules for registered CA key generation and protection, validated at level 3. Certificates shall be signed using a hardware cryptomodule that meets level 3.
6.2.2	Private key multi-person control	Multi-person control requires that more than one person (typically the registered CA and one or more separate security officers) independently authorize themselves to the system that will perform registered CA operations. This procedure shall prevent any single person (CA or otherwise) from gaining access to the registered CA signing key. Key management and end-entity signature keys may be backed up in multiple tokens without two-person control provided the operations to do so are audited and provided the private keys never exist in an unencrypted form outside the token. Registered CA signing keys shall be backed up only under two-person control. The employees who serve as the two-person control shall be identified in a list that shall be maintained by the registered CA and made available by the CA for audit.
6.2.3	Private key escrow	A signing key never shall be escrowed. For some purposes (such as data recovery), however, it will be necessary to provide key escrow and/or key recovery for confidentiality keys. The method for this shall be described in the CPS.
6.2.4	Private key backup	An entity optionally may back-up its own digital signature private key. If so, the key shall be copied and stored in encrypted form and protected at a level no lower than identified for the primary version of the key.
6.2.5	Private key archival	If a registered CA is acting as a key recovery agent, it shall archive private key management keys as part of its service. Private signature keys supporting non-repudiation services never shall be archived. A person optionally may archive his or her own private key.
6.2.6	Private key entry into cryptographic module	Private keys shall be generated and kept inside cryptographic modules evaluated to at least FIPS 140-1 level 3. If a private key is to be transported from one cryptomodule to another, the private key shall be encrypted during transport; private keys never shall exist in plain text form outside the cryptomodule boundary.
6.2.7	Method of activating private key	Private keys shall be activated by activation data stored securely and separately from cryptomodules.
6.2.8	Method of deactivating private key	Cryptomodules that have been activated shall not be left unattended or otherwise open to unauthorized access. After use they must be deactivated, *e.g.* by a manual logout procedure or by a passive timeout. Hardware cryptomodules shall be removed and stored or shall be within the registered CA's sole control when not in use.
6.2.9	Method of	Private keys shall be destroyed when they no longer are needed or when the

	destroying private key	certificates to which they correspond expire or are revoked. For software cryptomodules, destruction may mean overwriting the data. For hardware tokens, destruction may mean executing a zeroize command. Physical destruction of hardware is not required.
6.3	***Other aspects of key pair management***	A registered CA shall retain all verification public keys.
6.3.1	Public key archival	Each registered CA, authenticating RA and CMA shall protect its private key(s) in accordance with the provisions of this policy.
6.3.1.1	Key replacement	All keys shall have validity periods of no longer than twenty years. Suggested validity period: CA public verification key and certificate - twenty years; CA private signing key - eight years; end-entity public verification key and certificate - twelve years; end-entity private signing key - two years.
6.3.1.2	Restrictions on registered CA's private key use	The private key used by a registered CA for issuing certificates shall be used only for signing such certificates and, optionally, CRLs or other validation services responses. A private key held by an authenticating RA, if any, is considered the registered CA's private key and shall not be used by the authenticating RA for any other purpose, except as agreed by the registered CA and the authenticating RA. The private key used by each authenticating RA for the issuance of certificates shall be used only for communications relating to the approval or revocation of such certificates.
6.3.2	Use periods for the public and private keys	The key use periods for keying material are described in section 6.3.1.
6.4	***Activation data***	
6.4.1	Activation data generation and installation	A pass-phrase or PIN (activation data) shall be used to protect access to use of the private key. The activation data may be user selected. If the activation data must be transmitted, it shall be transmitted via a channel of appropriate protection, and distinct in time and place from the associated cryptomodule. If transmission is not accomplished by hand, the user shall be advised of the shipping date, method of shipping, and expected delivery date of any activation data. As part of the delivery method, users will sign and return a delivery receipt. In addition, users also shall receive (and acknowledge) a user advisory statement to help them understand responsibilities in the use and control of the cryptomodule.
6.4.2	Activation data protection	Activation data shall be memorized, not written down. Activation data never shall be shared. Data used for entity initialization shall be protected from unauthorized use by a combination of cryptographic and physical access control mechanisms. The private keys of entities shall be protected from unauthorized use by a combination of cryptographic and physical access control mechanisms. The level of protection shall be adequate to deter a motivated attacker with substantial resources. If a reusable password scheme is used, the scheme shall include a function to temporarily lock the account after a predetermined number of login attempts.
6.4.3	Other aspects of	This policy makes no provision for the life of activation data; however, it shall be

	activation data	changed periodically to decrease the likelihood that it has been discovered. Registered CAs shall define activation data requirements in their CPSs.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

All registered CA servers shall include the following functionality, either provided by the operating system or through a combination of operating system, PKI application and physical safeguards:

- access control to registered CA services and PKI roles;
- enforced separation of duties for PKI roles;
- identification and authentication of PKI roles and associated identities;
- object re-use or separation for registered CA random access memory;
- use of cryptography for session communication and database security;
- archival of registered CA and end-entity history and audit data;
- audit of security related events;
- self-test of security related registered CA services;
- trusted path for identification of PKI roles and associated identities;
- recovery procedures for keys and the registered CA system.

6.5.2 Computer security rating

A registered CA's equipment shall meet and be operated to at least a C2 [TCSEC] or E2/F-C2 [ITSEC] rating, or equivalent. A registered CA's equipment operating at a C2 equivalence shall, as a minimum, implement self-protection, process isolation, discretionary access control, object reuse controls, individual identification and authentication and a protected audit record.

6.6 Life cycle technical controls

Equipment (hardware and software) procured to operate a PKI shall be purchased using a process such as random selection, which will reduce the likelihood that any particular equipment has been subject to tampering. Equipment developed for a PKI shall be developed in a controlled environment, and the development process shall be defined and documented. Registered CA equipment shall be packaged securely and delivered using a defined procedure that records the actions of those involved. Tamper-evident packaging shall be used, or equipment shall be hand-carried from a controlled procurement environment to the installation site. The registered CA equipment shall be dedicated to administering a key management infrastructure. It shall not have installed applications or component software, which are not part of the registered CA configuration. Equipment updates shall be purchased or developed using the same random or like process as the original equipment and shall be installed by trusted and trained personnel in a manner defined in the CPS.

6.6.1 System development controls

A registered CA shall use CA software that has been designed and developed either under a development methodology such as MIL-STD-498, the system security

engineering capability maturity model (SSE CMM) or information systems security-engineering handbook. The design and development process shall provide sufficient documentation to easily facilitate third party security evaluation of the registered CA components and to easily facilitate: third party verification of process compliance; on-going threat risk assessments to influence security safeguard design and minimize residual risk.

6.6.2 Security management controls

A formal configuration management methodology shall be implemented for installation and ongoing maintenance of a registered CA system. The registered CA software, when first loaded, shall provide a method for the registered CA to verify that the software on the system: originated from the software developer; has not been modified prior to installation; and is the version intended for use. The registered CA shall have adopted and implemented procedures and policies to control and monitor the configuration of the registered CA system and to verify periodically the integrity of the software. At the time of installation, and at least once every 24 hours, the integrity of the registered CA system and software shall be validated using these procedures and policies.

6.7 Network security controls

Registered CA equipment shall not be connected to more than two network domains at a time. Registered CA equipment that is intended to connect to more than one network classification domain shall have procedures defined in a CPS which prevent information from one domain from reaching another (*e.g.*, equipment shutdown, removable hard drives, switching the network connection). Registered CA equipment may operate through a network guard provided it does not compromise the function of the guard. Protection of registered CA equipment shall be provided against known network attacks. Use of appropriate boundary controls shall be employed. All unused network ports and services shall be turned off. Only network software necessary to the functioning of the registered CA application shall be located on the registered CA equipment. Root registered CA equipment shall be stand-alone (off-line) configurations.

6.8 Cryptographic module engineering controls

Requirements for cryptographic modules are as stated above in section 6.2.

7 Certificate and CRL profiles

7.1 Certificate profile

Certificates that reference this policy shall contain public keys used for authenticating the sender of an electronic message and verifying the integrity of such messages –*e.g.*, public keys used for digital signature verification. All certificates that reference this policy will be issued in the X.509 version 3 format and will include a reference to the OID for this policy within the appropriate field. The CPS shall identify the certificate extensions supported, and the level of support for those extensions.

7.1.1 Version number and base fields

A registered CA shall issue X.509 Version 3 certificates, in accordance with the PKIX certificate and CRL Profile. The PKI end-entity software must support all the base (non-extension) X.509 fields:

Version — version of X.509 certificate, version 3(2)

Serial number — unique serial number for certificate as well as the certificate extensions defined in

		section 7.1.2
	Signature	CA signature to authenticate certificate
	Issuer	name of registered CA
	Validity period	activation and expiration date for certificate
	Subject	subscriber's distinguished name, which may contain additional numbers or letters appended to the common name to ensure the name's uniqueness within the domain of certificates issued by the registered CA
7.1.2	Certificate extensions	No extension shall modify or undermine the use of X.509 base fields. Additionally:
7.1.2.1	Certificate policies	The certificate policies field shall be populated in all certificates with one of the policy OIDs identified in section 1.2 and may be set as a non-critical extension.
7.1.2.2	Policy constraints	No provision.
7.1.2.3	Critical extensions	All entity PKI software shall correctly process critical extensions identified in this policy.
7.1.2.4	Supported extensions	The CPS shall define the use of any extensions supported by a registered CA, the authenticating RAs and end entities.
7.1.3	Algorithm object identifiers	Certificates issued pursuant to this policy shall use the following OIDs for signatures: id-dsa-with-sha1 {iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3} Certificates issued pursuant to this policy shall use the following OIDs for identifying the algorithm the subject key was generated for: encryption {iso(1) member-body(2) us(840) (113549) pkcs(1) pkcs-1(1) 1} publicnumber {iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1} Certificates containing keys generated for use with DSA or for use with KEA shall be signed with id-dsa-with-sha1. Keys generated for use with RSA shall be signed using sha-1WithRSAEncryption (1.2.840.113549.1.1.5). For alternate algorithms, only PMA-approved algorithms shall be used.
7.1.4	Name forms	Every DN shall be in the form of an X.501 printable string.
7.1.5	Name constraints	Subject and issuer DNs shall comply with PKIX standards and be present in all certificates.
7.1.6	Certificate policy object identifier	A registered CA shall ensure that the policy OID is contained within the certificates it issues.
7.1.7	Use of key use extension	A registered CA shall populate and mark as critical the key use extension in a certificate and identify the subscriber's private key as being used either for signing (digital signature and non-repudiation) or for encryption (dataEncipherment and keyEndipherment).
7.1.8	Policy qualifiers syntax and semantics	A registered CA shall populate the policy qualifiers extension with the URL of its CP.
7.2	***CRL profile***	If used, CRLs shall be issued in the X.509 version 2 format. The CPS shall identify the CRL extensions supported and the level of support for these extensions.

7.2.1	Version numbers	A registered CA shall issue X.509 version two (2) CRLs in accordance with the PKIX certificate and CRL profile.
7.2.2	CRL and CRL entry extensions	All entity PKI software shall process correctly all CRL extensions identified in the certificate and CRL profile. The CPS shall define the use of any extensions supported by the registered CA and end entities.

8 Policy administration

8.1	***Policy change procedures***	This policy shall be reviewed by PMA every year. Errors, updates, or suggested changes to this policy shall be communicated to the PMA contact on or before the date ninety days from the anniversary date of the day on which this policy becomes effective. Such communication shall include a description of the change, a change justification and contact information for the person requesting the change. The PMA shall review any notices of errors, updates or suggested changes and provide recommendations to ITEC and registered CAs. All proposed policy changes shall be disseminated to interested persons (see section 8.2) for a period of thirty days beginning sixty days prior to the anniversary date of the date on which this policy becomes effective (the review period). ITEC shall use its best efforts to accept or reject any proposed changes promptly upon the close of the review period. Notwithstanding, if, in the judgment of ITEC or the PMA, it is determined changes to the policy should be made prior to the annual review, ITEC reserves the right to modify the policy upon notification of the proposed changes to registered CAs. Registered CAs and authenticating RAs shall be given reasonable time to comment, and conform to the proposed changes.
8.1.1	List of items that may change without notification	Notice of all proposed changes to this policy that are considered by the state and a registered CA, which may materially impact users of this policy (other than editorial or typographical corrections, or changes to the contact details), shall be provided to authenticating RAs and shall be posted on the world wide web site of a registered CA. A registered CA shall post notice of such proposed changes in its repositories and shall advise subscribers in writing in tangible form or by e-mail of such proposed changes.
8.1.2	List of items subject to notification requirement	All provisions in this policy shall be subject to the notification requirement. Prior to the effective date of any changes to this policy, ITEC through the PMA shall notify all registered CAs and authenticating RAs.
8.1.3	Comment period, process and procedure	Affected users may file comments with the PMA within 30 days of the posting of the original notice. If the proposed change is modified as a result of such comments, a new notice of the modified proposed change shall be given.
8.2	***Publication and notification policies***	All registered CAs shall post a copy of this policy in electronic form on the internet.
8.2.1.1	Notification procedure	The PMA shall give written notice of any proposed changes to this policy to the secretary, registered CAs and authenticating RAs.
8.2.1.2	Procedure for	Written and signed comments on proposed changes shall be directed to the PMA.

	comments	Decisions on the proposed changes shall be at the sole discretion of the ITEC with the advice of PMA.
8.2.1.3	Final change notice	ITEC shall determine the period of time for notice of final change. `
8.2.2	Provisions for which change requires a new policy	If a policy change is determined by ITEC or the PMA to warrant the issuance of a new policy, the ITEC may require a new object identifier (OID) for the modified policy.
8.3	***CPS approval procedures***	When a registered CA's CPS contains information relevant to the security of the registered CA, that part of the CPS is not required to be made available publicly. In this instance, the PMA shall prescribe a method for confidential communication of the information it requires, and the registered CA shall provide it in that method. The information provided in this manner shall not be disclosed by the PMA unless it is determined that it does not qualify as information related to the security of the registered CA and, therefore, is not exempted under the Kansas open records act.
8.4	Waivers	Waivers from this policy will shall not be granted for any level of assurance. Variation in a registered CA's practice either shall be deemed compliant with this policy, or a change shall be requested to this policy.